Digital Safety Policy

Nominated Safeguarding Advisor: Rachel

Cleverton ICT coordinator: David Cunnelly

Date: November 2020

Shoreditch Park Primary School is a Rights Respecting School.

School policies respect the UN Convention on the rights of the child.

The Digital Safety Policy links to:

Article 13 Every child must be free to express their thoughts and opinions and to access all kinds of information

Article 16 Every child has the right to privacy.

Article 17 Every child has the right to reliable information… [and have] help protecting children from information which may be harmful

Contents

Linked policies:

- Positive Behaviour and Anti-Bullying Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy
- Information Sharing Policy

Statutory Guidance:

- Keeping Children Safe in Education 2020
- Working Together to Safeguard Children

Overview

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. Children and young people have an entitlement to safe internet access at all times. We understand and embrace the fact that technology is continually changing and the importance of schools staying up to date with new developments. For full details regarding the curriculum taught, please see the computing handbook which outlines throughout the year which strands of learning are covered through strands of Switched on Computing.

The requirement to ensure that pupils are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. The dangers they may face include:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online

(from Inspecting E-Safety in Schools, Ofsted January 2014)

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so they have the confidence and skills to face and deal with these risks. Shoreditch Park Primary School must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This policy explains how we intend to do this, while also addressing wider educational issues in order to help pupils (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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

Roles and Responsibilities

This section outlines the roles and responsibilities for E-Safety of individuals and groups within Shoreditch Park Primary school:

Governors: The Governing Body are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

Headteacher: The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the Nominated Safeguarding Advisor.

The Headteacher and Senior Leadership Team are responsible for:

- Ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- Ensuring there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role.
- Ensuring they receive regular monitoring reports from the E-Safety Co-ordinator.
- Ensuring that curriculum for computing is taught in accordance with the scheme of work (switched on computing) which develops coverage of E-Safety throughout the Key Stages.

The Headteacher and another member of the Senior Leadership Team should be aware of the Local Authority procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

The E-Safety Team:

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
- Attends relevant meetings / committee of the Governing Body
- Reports regularly to Senior Leadership Team

Technical Support Staff: It is the responsibility of the school to ensure their technical support company and technicians carry out any E-Safety measures, and that they are aware of this policy. Their role might include:

- Ensuring the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring the school meets the E-Safety technical requirements outlined by the LGfL and Local Authority guidance
- Ensuring users may only access the school's networks through a properly enforced password protection policy
- Ensuring the LGfL is informed of issues relating to the filtering applied by the Grid

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)(Appendix 1)
- They report any suspected misuse or problem to the E-Safety Co-ordinator (David Cunnelly) or Deputy Headteacher (Rachel Cleverton) for investigation, action or sanction
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school E-Safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities. This includes the use of iPads and Chromebooks to enhance learning.
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that they follow the procedure in place for dealing with any unsuitable material that is found in internet searches

Nominated Safeguarding Advisor: is aware of the potential for serious child protection issues that may arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues but the technology provides additional means for child protection issues to develop.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (Appendix 1), which they will be expected to sign before being given access to school systems**.**
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers: Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local E-Safety campaigns. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy if appropriate
- Endorsing (by signature) the Permissions Letter regarding their child's use of the internet and use of their child's images (Appendix 1)
- Accessing the school website and any on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users: Any users who access school ICT systems as part of the Extended School provision will be expected to sign an Acceptable Use Policy before being provided with access to school systems. (Appendix 1)

Online Learning

Please refer to the remote learning handbook which can be found **here** for information on how pupils are kept safe online in Google Classroom.

Mobile phones and digital technology

Mobile phones, iPads and digital technologies should be used in accordance to the criteria set out below by all staff and volunteers in school. Children are not to have mobile phones with them in school at any time, however their phones may be locked away (Year 5 / 6 classrooms) at the start of the day if needed to ensure a safe journey to and from school

Staff should not have personal mobile phones with them when they are working with children at the setting. These conditions also apply to students and volunteers.

Staff mobile phones must be kept in staff lockers and used only when staff are on break time in the staff room or outside the setting;

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

Parents, carers and visitors are requested not to use their mobile phones while on the school premises. School staff will remind parents, carers and all visitors of the policy by reminding them to switch off their phones when they enter the setting or asking them to leave the rooms to make or receive calls in the reception area/foyer when necessary.

Managing the Internet Safely

Security
The school will do all that it can to make sure the school network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information.
Digital communications, including email and internet postings, over the school network, will be monitored.

Policy and procedures

Shoreditch Park Primary School:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in areas where older pupils have more flexible access
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age or subject appropriate web sites
- Plans the curriculum context for Internet use to match pupils' ability, using child- friendly search engines where appropriate; eg kidrex, yahoo for kids or ask for kids
- Is vigilant when conducting 'raw' image or internet searches with pupils e.g. Google image search
- Informs users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the E-Safety Team.
- Requires all staff to sign an Acceptable Use Form, and keeps a copy on file (Appendix 1)
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the Permissions agreement form at time of their child's entry to the school
- Makes clear all users know and understand what the rules of appropriate use are, and what sanctions result from misuse – through staff meetings and in lessons for pupils
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system

- Ensures the named child protection officer has appropriate training
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides E-Safety advice for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities, e.g. the Police and/or the LA.

Education and training:

Shoreditch Park Primary school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable either in or out of school
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off their monitor and report it to the teacher / supporting adult
- Ensures pupils and staff follow the bullying policy in the case of any cyber bulling incidents.
- Ensures all pupils know how to report any abuse
- Has a clear E-Safety education programme throughout all Key Stages Pupils are taught a range of skills and behaviors appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search
    - to understand 'Netiquette' behaviour when using an online environment, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos
- to understand why they must not post pictures or videos of others without their permission
- to know not to download any files – such as music files - without permission
- to have strategies for dealing with receipt of inappropriate materials
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism, and that they must observe and respect copyright / intellectual property rights

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. For example, risks in pop-ups, buying things online

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection

- Ensures that parents are aware of responsible internet use and that the Computing lead / safeguarding lead provide workshops and opportunities to educate parents on safe internet usage. These workshops are to be open to all parents across the year to both educate and support in questions about internet usage; particularly with new technologies which may require filters. These workshops may be led by in school staff or outside agencies such as the NSPCC.

Homework through Google Classrooms

At Shoreditch Park Primary School homework is set through Google Classrooms for every year group. To access this, every child will have a unique log in email address for which the email function has been disabled.

In order to keep children safe, the following measures have been put in place:

- All comments boxes have been disabled to avoid inappropriate comments and constant moderation of forum
- Video chat options to be disabled at all times
- Children to sign acceptable use policy and create an online safety class charter in class through E-Safety lessons

In the event that a child breaches any of the agreements within the acceptable use policies, teachers will identify this and follow up with parents regarding appropriate communication. Teachers or Computing lead will at this point 'mute' children from being able to post at all online – with the exception of when posting work to their teacher.

For further guidance on how children are kept safe using Google Classroom, please see the remote learning handbook.

Use of digital and video images

At Shoreditch Park Primary School

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school
- Digital images /videos of pupils are stored in a private teachers' shared images folder on the network and images should be deleted at the end of the year – unless an item is specifically kept for a key school publication
- When using a staff or school iPad, pin codes must be used to keep all materials and images safe and secure.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils (Appendix 1)

- The school blocks access to social networking sites or newsgroups unless there is a specific approved educational purpose, for example with twitter.
- Pupils are taught about how images can be manipulated in their E-Safety education programme and are also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse. This further extends to children having an awareness that once on the internet, data

School Trips

At this time we are not embarking on school trips, but upon resumption it is the case that **NO pupils should carry their own mobile phones** or take photographs using their phones. The lead teachers will have mobile phones to use in the case of an emergency, but will only use school registered iPads to take photographs – not their own personal devices.

Parents accompanying classes on trips may take their own mobile phones and take photographs, but must be made aware that these images are for their private family use only and must not be shared on the Internet in any form e.g. via Facebook, as stated in the Parent Permission Forms

Website

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website administrators
- The school web site complies with the school's guidelines for publications
- Most material is the school's own work. Where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address: admin@shoreditchpark.hackney.sch.uk
- Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached

- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

Managing Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

All staff must agree to the terms and conditions of usage for iPads and these must not be taken off the premises.

Personal Devices

Staff are allowed to bring personal devices such as mobile phones, iPads etc. into school but must follow the rules set out in the Staff and Volunteer Acceptable Use Agreement. (Appendix 1)
Pupils should not have mobile phones or other personal devices in school. If any such devices are brought in they should be stored in the lockers in each class for safe-keeping at the beginning of the day, and collected at home time.

On school trips, NO pupil should carry their own mobile phones or take photographs using their phones. The lead teachers will have mobile phones to use in the case of an emergency, and will also carry digital cameras for taking photos. Staff are not to use mobile phones to take pictures of children or any personal device for doing so.

Parents accompanying classes on trips may take their own mobile phones and take photographs, but must be made aware that these images are for their private family use only and must not be shared on the Internet in any form e.g. via Facebook.

Policy and procedure

Shoreditch Park Primary School:

- Ensures staff read and sign that they have understood the school's E-Safety Policy. Following this, they are set-up with email and network access. Access is through a unique username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs[1]
- Maintains equipment to ensure Health and Safety is followed, for example our projector filters are cleaned by the site manager, equipment is installed and checked by approved Suppliers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role, for example the SEN Co-ordinator to access SEN data

[1] "'Use for private purposes' means any use that is not use in performing the duties of the employee's employment." HMRC EIM21613 Section 316(2) and (3) ITEPA 2003

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems, e.g. technical support
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school ICT systems regularly with regard to health and safety and security

What Do We Do If…

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child?

1. Play the situation down, don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians / and ensure the site is filtered
4. Inform the Local Authority

An inappropriate website is accessed <u>intentionally</u> by a child?

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the Local Authority if appropriate

An adult uses School IT equipment inappropriately?

1. As far a possible, ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).
    - Inform governors of the incident.

In an extreme case where the material is of an illegal nature:

- Contact the local police or High Tech Crime Unit and follow their advice.
- If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time?

1. Advise the child not to respond to the message.
2. Refer to relevant policies including E-Safety, anti-bullying and behaviour and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA E-Safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff?

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA E-Safety officer.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child?

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA E-Safety officer.
6. Consider delivering a parent workshop for the school community.

We foster a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material or situation that makes them feel uncomfortable.

Infringements

How will infringements be handled?

Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

How will staff and pupils be informed of these procedures?

- All staff are required to read and sign the school's E-Safety acceptable use agreement form (Appendix 1)
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'.
- The school's E-Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school (Appendix 1)
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on E-Safety issues (page 12)

Shoreditch Park Primary School

Staff and Volunteer Acceptable Use Policy Agreement

(Appendix 1)

Staff Acceptable Use Policy

This agreement covers the use of digital technologies in Shoreditch Park Primary including email, internet, shared network drives, network resources, all software, electronic equipment and all systems.

- I will only use Shoreditch Park Primary 's digital technology resources and systems for professional purposes
- I will not reveal my password(s) to anyone
- I will follow 'best practice' advice in the creation and use of my password(s). If my password is compromised, I will ensure I change it
- I will not use anyone else's password, nor seek to discover it. If a colleague does reveal it to me, I will advise them to change it
- I will not allow unauthorised individuals to access any of Shoreditch Park Primary 's systems
- I will ensure all documents and digital resources are saved, accessed and deleted in accordance with the Shoreditch Park Primary's network and data security and confidentiality protocols
- I will not engage in any online activity that compromises my professional responsibilities, code of conduct or professional boundaries
- My personal online communication tools, including mobile phones, will not be used with service users and I will not communicate or 'befriend' any service user using these methods, even if they have recently left or no longer use the service
- I will use only the approved email system for all email communication related to work at Shoreditch Park Primary
- I will not browse, download or send material that could be considered offensive to colleagues or others
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to Rachel Cleverton
- I will not download any software or resources that can compromise the network, that breach a user's copyright, or are not correctly licenced
- I will not publish or distribute work that is protected by copyright
- I will not connect a computer, laptop, notebook or other electronic device (including USB flash drive) to the network that does not have up-to-date anti-virus software
- I will not use personal digital cameras or camera phones for taking and transferring images of children/young people or staff/volunteers without written permission, and will use those images only for their intended purpose
- I will ensure that any personal social networking sites/blogs, Twitter, Instagram accounts, etc., that I create or actively contribute to are separate from my professional role
    - It is my responsibility to ensure that my use of social networking sites/blogs, etc., does not compromise my professional role, and will ensure my privacy settings are appropriate
    - Using such sites in work, on mobile devices or school computers is prohibited
- Any computer, laptop or electronic device loaned to me by Shoreditch Park Primary is provided solely for professional use

- I will access Shoreditch Park Primary's resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those resources
- Any confidential data that I transport from one location to another will be protected by encryption
- I will follow Shoreditch Park Primary's data security protocols when using confidential data at any location
- Any information seen by me with regard to service users held within Shoreditch Park Primary will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority, e.g. Children's Social Care and/or the police
- It is my duty to support a whole organisation safeguarding approach and I will alert the Shoreditch Park Primary's named child protection officer/relevant senior member of staff if the behaviour of any service user or member of staff/volunteer may be inappropriate or a cause for concern
- It is my responsibility to ensure that I remain up-to-date, read and understand the Shoreditch Park Primary's most recent online safety policies
- I understand that all internet/network usage can be logged and this information can be made available to my line manager on request
- I understand that failure to comply with any aspect of this agreement could lead to disciplinary action

I agree to abide by this Acceptable Use Policy at all times

I wish to have a network account; an email account; and be connected to all systems that are relevant to my post at Shoreditch Park Primary

Full name ..... (printed)

Job title .....

Signature ..... Date: .....

Authorized signature

I approve this user to be set-up on Shoreditch Park Primary's computer systems

Full name ..... (printed)

Job title .....

Signature ..... Date: .....

Use of encrypted memory sticks contract (Appendix 2)

Anything considered personal data MUST be saved and/or stored on an encrypted memory stick.

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents/carers e.g. **names**, **addresses**, contact details, legal guardianship contact details, health records, disciplinary records
- **Curricular/academic data e.g. class lists, pupil progress records or reports**
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

The school has provided staff with an encrypted memory stick for this purpose.

Please note:

The memory stick is the property of the school. If a member of staff leaves they must return the memory stick to the school before their final day.

It is the responsibility of the staff member to look after the memory stick. If the stick is lost or broken, they must inform the school immediately and they will be liable to pay for a new one.

Staff should ensure that personal data is not retained for longer than is necessary. Information should be deleted as soon as it is no longer required.

(For more details about the school's Data Protection Policy, please refer to the school's e-safety policy)

I have read and agree to the above conditions.

Name: _____

Signed: _____

Date: _____

Memory Stick serial number: _____

Parents/carers information and guidance (Appendix 3)

Online safety is concerned with safeguarding children in the digital world. We encourage you to learn how to use new technologies and ICT (Information Communication Technology) in a positive way.
Online safety is not about restricting children, but educating them about the risks as well as the benefits so they can feel confident, safe and happy online.
To keep your children safer online:

- ✓ Think about how you guide your family in the real world and do the same in the digital world - don't be afraid to set boundaries and rules for your children
    - Boundaries may be the amount of time children can spend on a computer, smartphone tablet or games console, along with the types of websites they can visit or which apps you allow them to download (remember to ensure young children cannot download apps themselves, and must always seek your authorisation before using an internet-connected device)
- ✓ Encourage balanced use – switching off devices at mealtimes and before bedtime.
- ✓ Talk to your child. Share the experience of using technology with them - and ask them to show you how they use technology
    - Encourage your child to talk to you about anything they see or experience online which upsets or disturbs them
- ✓ Talk to your friends, family and other parents about how they help their children to manage their digital world - you might pick up some interesting tips
- ✓ If your child reports a problem make sure you support them, report it or seek advice from family and friends you trust, or organisations such as Childline or the NSPCC
- ✓ Discuss the importance of keeping personal details private. Personal data means full name, address, mobile phone number, email address and school name
    - Remind children to be careful about uploading and sharing photographs. You must always ask permission before uploading or sharing a photograph of someone else or you may breach their right to privacy
- ✓ Use a child friendly search engine, such as: www.kidrex.org
- ✓ Agree the type of websites they can visit, and add those to your parental controls (on the computer or via your internet service provider)
- ✓ Agree which apps they can download to a smartphone or tablet. The minimum age for all social media sites is 13, so no primary school-age children should be accessing these services
- ✓ Visit www.internetmatters.org/controls/interactive-guide/ for practical advice on how to activate parental controls for all types of devices around the home
- ✓ Install antivirus software, filtering and firewalls for your home and mobile equipment
- ✓ Remember that filters and firewalls are not always 100% effective and sometimes things can get past them – so we still have to think about our safety
- ✓ Locate the computer/laptop in a family room and don't allow webcams to be used unless with your consent and always in a family room under supervision
- ✓ Save any abusive messages or inappropriate images for evidence purposes, and always report any such incident to an adult you trust, or organisations such as Childline, NSPCC or CEOP
- ✓ Be aware of how to report nuisance calls, text messages, emails and other communication

Parent/child Acceptable Use Policy

These rules will keep me safe and help me to be fair to others. As a child, I will respect these rules, with the support and guidance of my parents/carers, and staff at Shoreditch Park Primary

- I will only use the computers for purposes agreed by Shoreditch Park
- I will only use the internet when a trusted adult supervises me
- I will keep my logins and passwords secret
- If I see anything that upsets me or I receive a message I do not like, I will not respond to it and I will show an adult I trust
- I know I can always speak to an adult I trust if I see something on the internet that I don't understand or that upsets me
- I will not attempt to visit internet sites that I know are banned
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless an adult I trust has given permission
- I will only edit or delete my own files and not look at, or change, other peoples' files without their permission

Child Agreement

Name: .....

- I understand the agreement for using computers, the internet, email and online tools safely and responsibly
- I know the adults looking after me will help me to stay safe and check that I am using the computer to help me with my work

Signature: ..... Date: .....

Parent/carer Agreement

- I have read and discussed the agreement with my child and confirm that he/ she has understood what the rules mean
- I understand that the setting will use appropriate filtering and ensure appropriate supervision when using online and digital technologies
- I understand that occasionally, inappropriate materials may inadvertently be accessed and accept that the setting will endeavour to deal with any incident that may arise, according to policy
- I understand that whilst my child is using the internet and other online tools outside of the early years setting, that it is my responsibility to ensure safe and responsible use with the support of the setting

Name: .....

Signature: ..... Date: .....

Pupil Google Classroom Acceptable Use Agreement

This agreement covers the use of online forums for remote learning in the event of pupil/year group isolation or homework at Shoreditch Park Primary.

Young person's agreement:

- I will be responsible for my behaviour when using the internet during school time and use Google Classroom respectfully.
- I know during a class video call that I must act responsibly as a member of Shoreditch Park Primary.
- I will not comment inappropriately on Google Classroom. If I accidentally come across any comments I will report it immediately to an adult.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I understand that everything I write on Google Classroom can be viewed by anyone in school.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to a teacher at school or through Google Classroom.
- I understand that my internet use at school and on the Google Classroom will be monitored and logged and can be made available to teachers and parents. I understand that these rules are designed to keep me safe and that if I choose not to follow them, teachers at school may contact my parents/carers.

Full name ..... (printed)

Google Classroom Email: ……

Signature ..... Date: .....