

# **ONLINE SAFETY & ACCEPTABLE USE POLICY**

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy. This policy applies to all staff, governors, volunteers, children and young people and anyone involved in activities at Old Palace Primary.

Online Safety encompasses Internet technologies and electronic communications, such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

## **Aims**

- Set out expectations for all Old Palace Primary School's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy, Anti-Bullying Policy, Remote Learning Policy)

## **Why is internet use important?**

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Access to the internet is therefore an entitlement for pupils, who show a responsible approach to its use. Our school has a duty to provide pupils with quality internet access and to teach them how to evaluate internet information and how to take care of their own safety and security online.

## **What are the risks for our school community?**

These can be summarised as:

### **Conduct**

- privacy issues, including disclosure of personal information;

- digital footprint and online reputation;
- health and well-being (amount of time spent online and gaming);
- sending and receiving of inappropriate and personally intimate images;
- copyright – not respecting ownership of intellectual property, for example plagiarism or illegal file sharing of music and film).

- **Content**

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

### Contact

- Online grooming through the internet, such as chat rooms, gaming and social networking sites.
- Cyber bullying in all forms.
- identity theft (including hacking profiles) and sharing passwords;

### Commercialism

- Exposure to advertising and marketing schemes (especially through gaming) meaning inadvertently spending money online.
- Spam emails and pop ups containing offers.
- Gaining access to personal information stored on the computer, mobile or games console and passing it on.
- Unintentionally enabling viruses and spyware on an electrical device.

	<b>Content</b> Child as recipient	<b>Contact</b> Child as participant	<b>Conduct</b> Child as actor	<b>Contract</b> Child as consumer
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
<b>Sexual</b>	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
<b>Values</b>	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
<b>Cross-cutting</b>	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

### Who is responsible for Online Safety?

All members of the school community have a responsibility to keep pupils safe online.

This includes staff, pupils, governors, volunteers, parents / carers and visitors who have access to the school's IT systems and devices, both in and out of school. Appendix H sets out the specific responsibilities associated with members of the school community.

All members of the school and wider community are encouraged to be vigilant in reporting issues, so these can be dealt with quickly and sensitively, using the processes outlined in the Child Protection Policy. The Designated Safeguarding Lead will handle any referrals made to MASH (Multi Agency Safeguarding Hub).

## **Educating parents about Online Safety**

Schools raise parents' awareness of internet safety in newsletters or information via the school website, workshops and the Online Safety Team. If parents have any queries or concerns in relation to online safety, these are addressed in the first instance by the Year Group Lead. If parents require support setting up safety features on their devices, they can book an appointment with the ICT technician via the Parent Support Workers.

## **How are pupils taught about safety online?**

The school has a clear, progressive Online Safety education programme as part of the Computing and PSHE curriculum, which has been developed using LGfL e--Safeguarding and national guidance. Internet use is carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas. A range of skills and behaviours, appropriate to age, are taught to pupils including:

- To apply the Top Tips (KS1) and Smart Rules (KS2) to keep safe online
- To understand why online '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 never give out personal details of any kind which may identify them and / or their location. Examples would include full name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- To know what to consider before placing personal photos on any social network space, for example damage to personal reputation or providing location details through background detail.
- To understand the importance of turning on privacy settings and ways to deny access to unknown individuals and to block unwanted communications
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site or web/blog page may have a particular bias or purpose and to develop skills to recognise what this may be;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand acceptable behaviour when using an online environment or email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand that permission should be sought before posting photographs or videos of others;
- To know not to download any files without permission;
- To understand the issues around aspects of the commercial use of the internet, such as clicking on pop-ups or making purchases online as well as online gambling;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand the impact of cyberbullying and trolling and know how to seek help if they are affected by any form of online bullying.
- [for older pupils] to understand why and how some people will 'groom' young people to form an unhealthy relationship;
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or CEOP.

In KS2, each class also nominates two Online Safety monitors who are trained by the Computing Lead to further understand the importance of Online Safety and use this knowledge to promote the SMART rules

and Top Tips to their peers. They have an on-going role to use our VLE to encourage, respond to comments and advise their peers.

## **How are IT systems managed to support Online Safety?**

### **Authorised Internet Access**

- The school uses individual, audited log-ins for all users; maintaining a record of all staff and pupils who are granted Internet access;
- All staff must read and sign the 'Acceptable Use Policy before using any school ICT resource (see appendix B)
- All pupils sign an Acceptable Use Agreement, agreeing to follow the school's Online safety rules;
- Guest accounts are available for visitors to the school, which allow limited access to the network. When using these accounts, visitors are required to accept the schools Acceptable Use Policy on the homepage
- The school is vigilant in its supervision of pupils' internet use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Parents consent to pupils accessing the internet as part of the Home School Agreement (see Appendix E).

### **Internet Security and Filtering**

- Ensures staff read and sign that they have understood the school's Acceptable Use Policy. Following this, they are set up with Internet and email access and can be given an individual network/email login username and password
- Provides pupils with an individual network login username and password
- Makes it clear that staff must keep their login details private
- Makes clear that pupils should never be allowed to logon or use teacher and staff logins
- Makes clear that no one should log on as another user
- Requires all users to always log off when they have finished working or lock their computers if they are leaving the computer unattended
- If a user finds a logged on machine, they must always logoff and then logon again as themselves
- Has setup the network so that users cannot download executable file/programs
- Uses a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.
- Has blocked access to sites which it considers may pose a risk to pupils
- Has blocked access to chat sites, social networking, music/film download and shopping sites – except those approved for educational purposes
- Requires staff to preview websites before use [where not previously viewed or cached] and to use child-friendly search engines where more open Internet searching is required e.g. Google Safe Search for Kids. Where Youtube clips are used, staff must check the comment section beforehand and ensure the chat box is disabled.
- Ensures pupils only publish within an appropriately secure environment.
- Maintains equipment to ensure Health and Safety is followed, e.g. projector filters cleaned by Network Manager, equipment installed and checked by approved Suppliers/LA electrical engineers
- Only allows remote access by staff through school and LA approved systems, such as google drive.

- 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 or MIS Support
- Uses the LGfL USO FX website for all CTF files sent to other schools
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure systems such as Egress and USO.
- 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. Servers are located in lockable rooms and are managed by DBS checked staff
- Disposal of equipment complies with the WEEE directive: an approved or recommended disposal company is used where any protected or restricted data has been held and a certificate of secure deletion required
- Ensures staff understand that any failure of the filtering systems must be reported directly to the Computing Lead. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary; any material we suspect is illegal is reported to the appropriate authorities
- Reviews the school ICT systems regularly with regard to security

## **Email**

Staff at Old Palace use the StaffMail system for all school emails. This system is linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.
  - Internally, staff should use the school network, including when working from home when remote access is available via G Suite.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- Personal e-mail addresses must not be accessed during teaching hours. These may be accessed before/after school and during designated breaks, providing pupils are not in the room

### **Pupils must:**

- Only use approved LGfL e-mail accounts on the school system;
- Immediately tell a teacher if they receive offensive e-mail;
- Not reveal personal details of themselves or others in e-mail communication;
- Not arrange to meet anyone without specific permission;
- Seek authorisation to send an e-mail to an external organisations;
- Not forward chain letters/emails.

### **Social Networking**

- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to pupils at the school.
- Use of social networking applications for personal use is not permitted on work devices. These may be accessed on personal devices, such as mobile phones, during designated breaks. School staff will ensure that in private use:
  - They do not engage in online discussion on personal matters relating to members of the school community. This includes making reference to pupils, parents and staff on social media
  - Personal opinions should not be attributed to the school or local authority
  - Security settings on personal social media profiles should be regularly checked to maintain privacy and to minimise the risk of loss of personal information. Training is provided to support this.

### **School Twitter**

- School twitter accounts are monitored daily to ensure comments and tags are appropriate and accurately reflect the school.
- Notifications are enabled on schools twitter accounts so that staff monitoring the account are aware of the activity on the account to ensure it is in line with schools policy.
- Inappropriate comments or tags will be removed immediately and users will be blocked from seeing the school account.
- The School has a record of consent by the parents for pupils who are allowed to be shown on the schools twitter page, for those children who do not have consent, images of the children will not be displayed or will have the child's identity concealed (for example their faces being covered).
- Posts will not include personal information about the children, including their names or academic attainment.
- Pupils will not be given access to the schools twitter accounts, any tweeting done on the class pages and main school twitter will be done by the designated staff members.
- Teachers may share class and school twitter pages with the class, but should open the page and remove any non-age appropriate advertising before sharing with the pupils.

### **Pupils:**

- Will not be allowed access to social networking sites except those that are part of an educational network or approved Learning Platform;
- Will be advised never to give out personal details or place personal photos of any kind which may identify them or their location;
- Will be taught how to deny access to unknown individuals and instructed how to block unwanted communications;
- As most social networks e.g. Facebook, state users must be over 13 years old to sign up for an account, we will not promote nor allow their use by pupils at Old Palace

### **Video Conferencing**

- Only LGfL supported services will be used for video conferencing activity;
- Only approved or checked webcam sites will be used;
- The use of video chat programs and apps e.g. Zoom are only allowed in monitored environments and then only to communicate with trusted, approved recipients.

### **Pupils:**

- Should ask permission from the supervising teacher before making or answering a video conference call.

- Please refer to the Remote Learning Policy for further guidance on safety.

### **Digital Images & Videos**

- Videos and photographs of children and adults from Old Palace are included on our website, twitter account and in the school newsletter, so parent and carers can view these at home and share them with family and friends. We also use photos of our pupils for our display boards.
- Permission for use of each child's digital photographs/ video is sought from parents/carers at the admission interview and forms part of the home school agreement;□
- We do not include the full names of pupils in a photograph or when showcasing examples of their work.
- When showcasing school-made digital video work, we take care to ensure that pupils are not referred to by name on the video, and that pupils' full names are not given in credits at the end of the film
- Personal details or geotags will never be embedded in or tagged to digital images/videos.
- Children's names are not used within file names.
- Where possible group photos/ videos will be taken, rather than those of individual pupils.
- Digital images / video of pupils must be stored securely on the school network and not on personal devices.
- Housekeeping ensures that images which no longer needed are removed at least annually
- Under no circumstances should images of pupils be posted online, other than on the school website or twitter page (with parental consent)
- Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection

### **Cloud Environments**

- Uploading of information on the schools' online learning space is shared onto the Staff Google Drive;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

### **School Website**

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our authorised website administrators
- The school website complies with the statutory DfE 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;
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. [admin@oldpalace.towerhamlets.sch.uk](mailto:admin@oldpalace.towerhamlets.sch.uk). Home information or individual email identities will not be published;

### **School iPads**

All teaching staff are allocated their own iPads as a tool to enhance classroom practice. This is not intended for personal use. The following procedures are in place:

- Before being assigned an iPad to a member of staff they must read and sign the 'iPad Loan Agreement' (Appendix G)
- Staff must bring the iPad to school every day and ensure that this is stored securely, both on and off site; Staff must ensure the device is always password protected;



- Regular equipment checks are carried out to ensure that iPads are being used for the intended purpose and have not been used to access or download inappropriate content.

## **What is the school's policy on the use of personal hand held devices and mobile phones?**

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying. Below we set out what is 'acceptable' and 'unacceptable' use of mobile phone and handheld devices by the whole school community (pupils, staff and visitors) while they are at school or undertaking school activities off site.

### **General issues**

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Staff and all visitors to the school are requested to keep their phones on silent/non vibrate.
- The sharing functions of a device should be switched off at all times and not be used to send images or files to other mobile phones.
- Devices may not be added to school wireless connection
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site. These include: toilets, areas where pupils are changing for PE and the school house.

### **Staff**

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Staff should store their devices in personal lockers or stock cupboards and use them only in designated break times unless prior permission has been given by the Headteacher. They should only be used in classrooms when pupils are not present.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Personal numbers should not be shared with children or parents.
- Personal mobile devices should never automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox etc).
- Staff should avoid using personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose. If personal equipment is being used for this purpose, for example during a residential visit, the device should be registered with the school on the undertaking that the photographs are only used for approved school business and will be transferred to the school network as soon as practically possible, and will not be stored at home or on memory sticks.
- If videos or images are taken for school purposes they should be transferred to the school network at the end of the school day and then be permanently deleted from the device
- Staff members can use a personal mobile phone during school visits in the event of an emergency to contact the school office or the emergency services.
- If a member of staff breaches the school policy then disciplinary action may be taken.

### **Pupils**

If pupils bring in their mobile phones, they should hand them in in the office at the beginning of the day and collect them back at the end of the day

## **Parents**

- Parents are requested not to use any mobile devices within the school grounds and building.
- Parents must not use their mobile devices during assemblies and other supervised special events, for the purpose of taking photographs or filming. An opportunity for staged photographs will be provided at the end of the performance, under the supervision of the teacher.
- Performance assemblies are filmed and posted on the school website so this can be shared with families.

## **How is personal data protected?**

- Personal data will be recorded, processed, transferred and made available according to GDPR, tailored by the Data Protection Act 2018. Please refer to the school's Data Protection Policy

## **How does the school handling Online Safety Concern or Complaints?**

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Protection & Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

Old Palace commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school) or during extended periods away from school. All members of the school are encouraged to report issues swiftly via CPOMS, alerting the DSL, Computing Lead and Year Group Lead to allow it to be dealt with quickly and sensitively.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead immediately.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the DSL and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

Any inappropriate websites or material found by pupils or staff will be reported to the Computing Lead who in turn will report to the Internet Service Provider (See Appendix A).

Complaints of Cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting as stated in the CP Policy).

If an incident were to take place during remote learning, please follow the guidance in the Remote Learning Policy.

## **How is this policy communicated?**

A copy of this policy is available on the school website. In addition:

### **Staff**

- Staff training in safe and responsible Internet use, data protection and Online Safety will be provided to all staff including administration, premises, governors and volunteers. Annual Online Safety training will take place, alongside the Child Protection Training at the start of every academic year.
- As part of the induction process, all new staff (including volunteers) are provided with information and guidance on the school's e-Safeguarding and Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Governors receive updates on Online Safety through the head teacher's termly report and this is a standing agenda item at Curriculum Committee Meetings.

### **Pupils**

- Online-safety posters are displayed by the computer in the classroom as well as around the school (Appendix F)
- Pupils will be taught online safety through the school's Computing & PHSCE curriculum.
- Safer Internet day will be celebrated annually through the use of special activities
- Pupils will be informed that Internet use will be monitored;
- Pupils sign an AUP (Appendix C)

### **Parents**

- Online safety, access to the internet and use of digital images are discussed with parents at their child's admission interview
- The school website and newsletters remind parents of the importance of online safety. Parent workshops are provided throughout the year.
- Parents sign an AUP (Appendix D)

A range of sites provide more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about online safety. At the time of writing these include:

The UK Safer Internet Centre website: <http://www.saferinternet.org.uk>

CEOP's Thinkuknow website: <http://www.thinkuknow.co.uk>

<http://www.thinkyounow.co.uk/parents>

Internet Matters: <http://www.internetmatters.org>

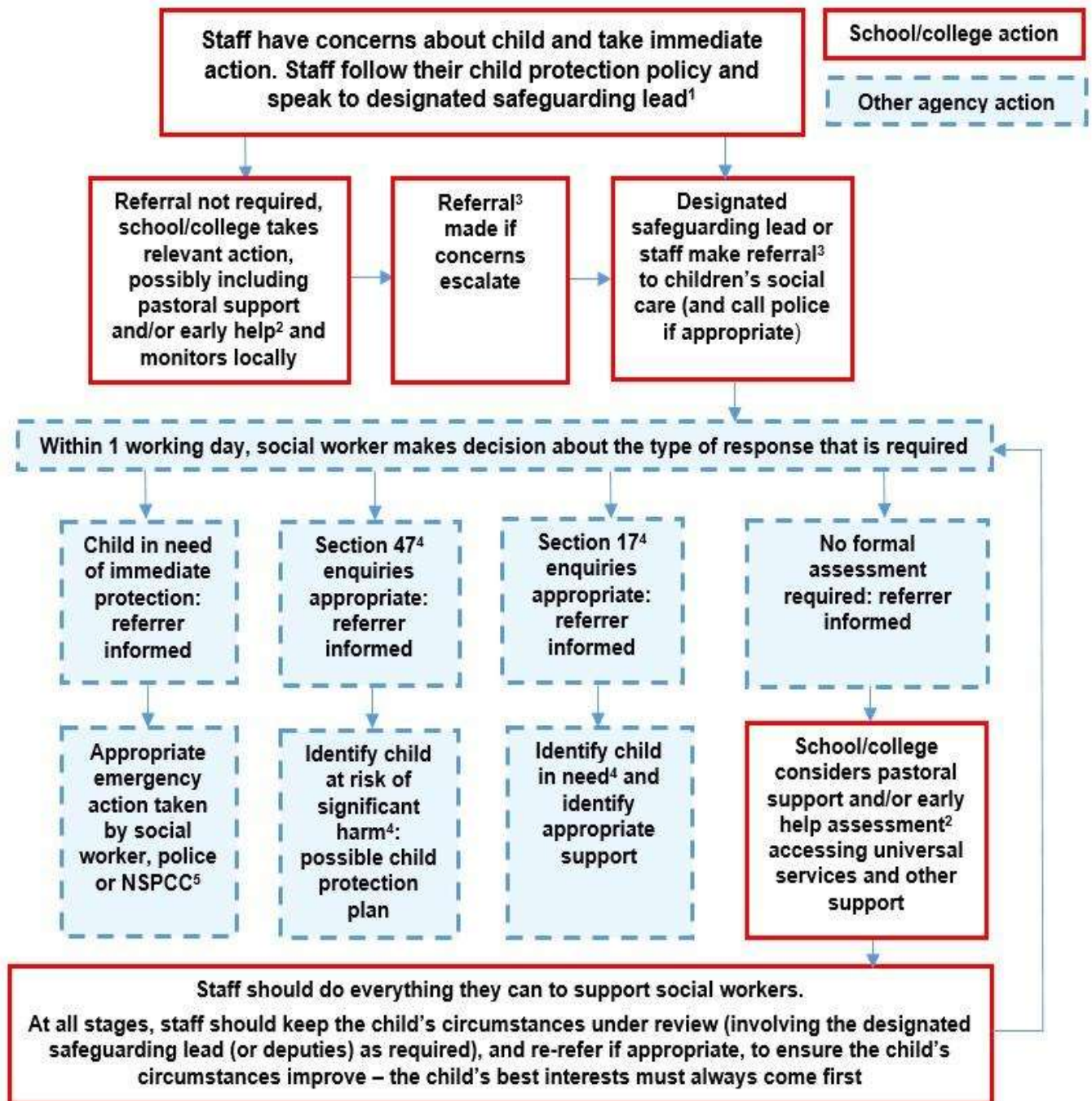
Childnet: <http://www.childnet.com/sns>

NSPCC: <http://www.nspcc.org.uk/onlinesafety>

Parent Zone: <http://www.parentzone.org.uk>

Ask About Games (where families make sense of video games): <http://www.askaboutgames.com>

**Appendix A**



## Appendix B

# Acceptable Use Policy (AUP) for **STAFF, GOVERNORS, VOLUNTEERS**

### What am I agreeing to?

1. (This point for staff and governors): I have read and understood Old Palace's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult).
3. **During remote learning:**
  - **I will not behave any differently** towards pupils compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
  - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
  - **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
  - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom. The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
  - **I will complete a CPOMs incident and alert the Yr group Lead, DSL and Computing Lead for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students
4. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
5. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum**, as well as safeguarding considerations when supporting pupils remotely.
6. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
7. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
  - not sharing other's images or details without permission
  - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
8. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways. If contacting parents/carers by email, this will be sent via the admin account. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.
10. I understand the importance of upholding my online reputation, my professional reputation and that of the school, and I will do nothing to impair either. I will ensure my personal opinions are not attributed to the school.

- 11. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords. I will only use complex passwords and not use the same password as for other systems.
- 12. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- 13. I will not install any software or hardware without permission.
- 14. I understand that school information and reprographic systems may not be used for private purposes.
- 15. I will respect copyright and intellectual property rights.
- 16. I will preview sites before use with pupils.
- 17. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
- 18. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
- 19. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
- 20. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
- 21. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

**To be completed by the user**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

I approve this user to be allocated credentials for school systems as relevant to their role.

**Any Additional permissions (e.g. admin)** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Appendix C

# Acceptable Use Policy (AUP) for KS1

**These statements can keep me and others safe & happy at school and home**

My name is \_\_\_\_\_

To stay **SAFE online and on my devices**

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**



8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to

9. I don't change **CLOTHES** or get undressed in front of a camera

10. I always check before **SHARING** personal information

11. I am **KIND** and polite to everyone



**My trusted adults are:**

\_\_\_\_\_ at school

\_\_\_\_\_ at home



# Acceptable Use Policy (AUP) for KS2

## These statements can keep me and others safe & happy at school and home

1. **I learn online** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. **I learn even when I can't go to school(remote learning)**– I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. **I ask permission** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. **I am creative online** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. **I am a friend online** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. **I am a secure online learner** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. **I am careful what I click on** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. **I ask for help if I am scared or worried** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. **I know it's not my fault if I see or someone sends me something bad** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. **I communicate and collaborate online** – with people I already know and have met in real life or that a trusted adult knows about.
11. **I know new online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. **I check with a parent/carer before I meet an online friend** the first time; I never go alone.
13. **I don't do live videos (livestreams) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. **I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. **I say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. **I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. **I follow age rules** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
18. **I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. **I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~  
**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at school that includes**

\_\_\_\_\_

**Outside school, my trusted adults are** \_\_\_\_\_

I know I can also get in touch with [Childline](#)

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Acceptable Use Policy (AUP) for Parents

### What am I agreeing to?

1. I understand that Old Palace uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others.
5. I will model appropriate behaviour when using social media and will not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's policy on the use of digital images and video, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety, read information provided by the school and access recommended sites and workshops which will support me to keep my child safe by providing suitable supervision, by setting parental controls, by limiting screen time (see Digital 5 A Day: [childrenscommissioner.gov.uk/our-work/digital/5-a-day/](http://childrenscommissioner.gov.uk/our-work/digital/5-a-day/) ) and by discussing with my child which content it is appropriate to access and share.
8. I understand that my child needs a safe and appropriate place to do remote learning if my child's class is closed. When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
9. If my child has online tuition, I will refer to the [Online Tutors – Keeping children Safe](#) poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet.

*Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. [swiggle.org.uk](http://swiggle.org.uk) and YouTube Kids is an alternative to YouTube with age appropriate content.*

11. I will support my child to adhere to the commitments made by them signing the Acceptable Use Policy (AUP) which s/he has signed, a copy of which can be seen in the Online Safety Policy appendix and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
12. I can find out more about online safety at Old Palace by reading the full Online Safety Policy on their school website and can talk to the class teacher or year leader if I have any questions or

concerns about my child/ren's safe use of technology, or about that of others in the school community.

~~~~~

**I/we have read, understood and agreed to this policy.**

**Signature/s:** \_\_\_\_\_

**Name/s of parent / carer:** \_\_\_\_\_

**Child's Name:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Old Palace Internet Access and Use of Children's Work and Images

### Parent's Consent for Internet Access

At Old Palace School we believe that the Internet is an essential part of your child's learning. The school provides Internet access to pupils and has very clear SMART rules (see other sheet) on how this access will be made as safe as possible.

We use the LA approved Internet provider and there is a filtering process in place which restricts access to inappropriate materials. We have a comprehensive *Online Safety and Acceptable Usage Policy* for all parents(attached). Pupils and staff are available on the school website should you require more details.

- **I give permission for my child to have access to the internet and agree that the school is not liable for any damages arising from use of the internet facilities.**
- **I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials and that the school cannot be held responsible for the nature or content of materials accessed through the Internet.**

### Parent's Consent for Use of Children's Work and Images

From time to time we take photographs, videos or audio recordings of children taking part in educational activities which may be included on school displays and celebrations of the pupils' work, on our school website, Twitter and on documents relating to the school, for example our school prospectus. In such instances, details of the pupil's full name will not be printed in conjunction with these images, videos or audio recordings. We allow parents to bring in photographic equipment into school, including mobile phones with cameras for the sole purpose of photographing school assemblies, trips and other supervised school activities. Video recording is not permitted.

- **I give permission for my child's photograph, video or audio recording to be used on school displays and celebrations of the pupil's work, on the school website and in publications relating to the school.**
- **I agree not to make video recordings on the school site.**






✂.....

**Please cut and return this part to the class teacher**

		Tick below ✓:
I have read and understand the SMART online Safety rules		
I give permission for my child to have access to the internet and agree that the school is not liable for any damages arising from use of the internet facilities		
I give permission for my child's photograph, video or audio recording to be used		
<b>Signed by parent/carers</b>	<b>Date:</b>	
<b>Name of child:</b>	<b>Class:</b>	

# e-Safety SMART Rules

When using the computer and internet we need to follow these e-Safety SMART rules:

 <p><b>SAFE</b></p>	<p>Keep <b>SAFE</b> by asking permission before using the internet, going onto any website or opening unknown files/emails.</p> <p>Do not give out personal information such as your phone number, your real name, your school name or password to anyone online.</p>
 <p><b>MEETING</b></p>	<p><b>MEETING</b> someone from the internet can be dangerous. Only do so with your parents' or carers' permission and only when they are there with you.</p>
 <p><b>ACCEPTING</b></p>	<p><b>ACCEPTING</b> emails, chat messages, or opening files or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!</p>
 <p><b>RELIABLE</b></p>	<p>Think 'How <b>RELIABLE</b> is it?'</p> <p>Some information on the internet may not be true. People you meet online may lie about themselves.</p>
 <p><b>TELL</b></p>	<p><b>TELL</b> your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.</p>

# e-Safety Top Tips

When using the computer and internet we need to follow these e-Safety Top Tips:

<b>Top Tip</b> <b>1</b>	People you don't know are strangers.  They're not always who they say they are.
<b>Top Tip</b> <b>2</b>	Be nice to people on the computer like you would in the playground.
<b>Top Tip</b> <b>3</b>	Keep your personal information private.
<b>Top Tip</b> <b>4</b>	If you ever get that 'uh oh' feeling, you should tell a <u>grown-up</u> you <u>trust</u> .

## Appendix G

### Old Palace iPad Loan Agreement Staff

ipad Make/Model	
ipad Serial Number	

#### 1. This agreement is between:

1) Old Palace Primary School, St Leonard's Street, London, E3 3BT ("the school")

2) Name of Staff: \_\_\_\_\_

Address: \_\_\_\_\_

This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

- The school is lending the Staff an iPad ("the equipment") for the purpose of doing work.
- This agreement sets the conditions for taking an Old Palace iPad ("the equipment") home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I will adhere to the terms of loan.

#### 1. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued.

- I understand that I am responsible for the equipment.
- If the equipment is damaged, lost or stolen, I will immediately inform the school office, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment.
- If the equipment is stolen, I will also immediately inform the police.
- I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.
- I will not leave the equipment unsupervised in unsecured areas.

#### 2. User Responsibility

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.
- Users must use protective cases/covers for their iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extremes of temperature.
- Do not store or leave unattended in vehicles.



- School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad. The iPads must not be loaned to other adults without agreement from the headteacher; ☒
- Users are encouraged to set a passcode on their iPad to prevent other Users from misusing it.
- Users will set up an iTunes account using their work email account;
- Any additional apps or media Users wish to purchase can be done through their own Teacher Apple iTunes account for a single licence; or the School's Volume Purchasing Programme. If a class set is required, a request will need to be sent to the Computing Lead. These apps will remain the property of the school.

**Safeguarding and Maintaining as an Academic Tool**

- Use of photographs of children must be in line with the Consent Letter Agreement. Permission is requested in the Home School Agreement for new arrivals.
- Any photographs taken of pupils should be transferred to the school network and then deleted by the end of the school day.
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.
- If a User requires a class set of apps or media, a request will need to be sent to the Computing Lead. The apps will be purchased using the School's Volume Purchasing Programme. These apps will remain the property of the school.

**Prohibited Uses**

- All material on the iPad must adhere to the Online and Acceptable Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- The iPad is a school tool designed to enhance classroom practice. It is not for personal use e.g. Facebook or social networking sites.
- Jailbreaking is the process which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.

**Lost, Damaged or Stolen iPad**

If the iPad is lost, stolen or damaged, the Computing Lead or Head Teacher must be informed immediately

Return date

I will return the device and accompanying charger in its original condition and box to the school office within 7 days of being requested to do so.

Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

<b>DATE</b>	
<b>STAFF MEMBER NAME</b>	
<b>STAFF MEMBER SIGNATURE</b>	
<b>DATE</b>	
<b>DATE RETURNED</b>	
<b>DEVICE CHECKED BY</b>	

## Appendix H

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> <li>● Support safeguarding leads and technical staff as they review protections for <b>pupils in the home</b> and <b>remote-learning</b> procedures, rules and safeguards (see <a href="https://remotesafe.lgfl.net">remotesafe.lgfl.net</a> for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology.</li> <li>● Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding</li> <li>● Ensure that the DSL responsibilities listed in the section below are being followed and fully supported</li> <li>● Ensure that policies and procedures are followed by all staff</li> <li>● Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships</li> <li>● Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information</li> <li>● Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information</li> <li>● Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles</li> <li>● Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles</li> <li>● Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident – report on CPOMs</li> <li>● Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised</li> <li>● Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures</li> <li>● Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety</li> <li>● Ensure the school website meets statutory requirements (see appendices for website audit document)</li> </ul>

Designated  
Safeguarding  
Lead (DSL)

- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology)
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy ( alongside the Computing Lead), other online safety documents (e.g. Acceptable Use Policies).
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents.
- Communicate regularly with SLT and other stakeholders to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident – by reporting on CPOMs.
- Ensure the updated [2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges](#) Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages at [kcsietranslate.lgfl.net](https://kcsietranslate.lgfl.net)
  - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
  - all staff to have Online Safety training, alongside CP training at the start of the academic year.

All Staff

- Understand the safeguarding provisions for **home-learning** and **remote-teaching technologies**.
- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are Alison Milward and Richard Lampard
- Read Part 1, of Keeping Children Safe in Education.
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures – reporting on CPOMs.
  
- Sign and follow the staff acceptable use policy
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum.
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues

	<ul style="list-style-type: none"> <li>● Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this <a href="#">Online Reputation</a> guidance for schools.</li> </ul>
<p>Computing Lead/Online Safety Lead (OSL)</p>	<ul style="list-style-type: none"> <li>● As listed in the ‘all staff’ section, plus:</li> <li>● Ensures that Online Safety education is embedded across the curriculum</li> <li>● Promotes an awareness and commitment to e-safeguarding throughout the school community, using events such as Safer Internet Day to reinforce this work</li> <li>● Devises and delivers training to all staff, including the procedures that need to be followed in the event of an Online Safety incident</li> <li>● To monitor the use of the technology and the school network (including google drive, remote access and email) in order that any misuse or attempted misuse can be identified and addressed</li> <li>● Liaises with the Local Authority and national agencies as appropriate</li> <li>● Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum</li> <li>● Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach</li> <li>● Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing</li> <li>● Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements</li> </ul>
<p>Governors</p>	<ul style="list-style-type: none"> <li>● Approve this policy and strategy and subsequently review its effectiveness.</li> <li>● Ask about how the school has reviewed protections for <b>pupils in the home</b> and <b>remote-learning</b> procedures, rules and safeguards.</li> <li>● Support the school in encouraging parents and the wider community to become engaged in online safety activities</li> <li>● Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings</li> <li>● Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised</li> <li>● Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information</li> <li>● Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children.</li> <li>● Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.</li> <li>● Ensure appropriate filters and appropriate monitoring systems are in place.</li> <li>● Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.</li> </ul>

Network Manager/ technician	<ul style="list-style-type: none"> <li>● As listed in the 'all staff' section, plus:</li> <li>● Support the HT and DSL team as they review protections for <b>pupils in the home</b> and <b>remote-learning</b> procedures, rules and safeguards (see <a href="https://remotesafe.lgfl.net">remotesafe.lgfl.net</a> for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology).</li> <li>● Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant</li> <li>● Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy</li> <li>● Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc</li> <li>● Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the senior leadership team</li> <li>● Maintain up-to-date documentation of the school's online security and technical procedures</li> <li>● To report online-safety related issues that come to their attention in line with school policy</li> <li>● Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls</li> <li>● Work with the Headteacher to ensure the school website meets statutory DfE requirements</li> </ul>
Data Protection Officer	<ul style="list-style-type: none"> <li>● Acts as the schools designated data controller</li> <li>● Ensures that all data held on pupils on the school office machines have appropriate access controls in place</li> <li>● Maintains records of signed acceptable use policies, ensuring these are received from new members of staff</li> <li>● Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.</li> <li>● Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>● To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts</li> </ul>
All Pupils	<p>Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually.</p> <ul style="list-style-type: none"> <li>● Treat <b>home learning during any isolation/quarantine or bubble/school lockdown</b> in the same way as regular learning in school and behave as if a teacher or parent were watching the screen</li> </ul>

	<ul style="list-style-type: none"> <li>● Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors</li> <li>● Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor</li> <li>● Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.</li> <li>● To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media</li> <li>● Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.</li> </ul> <p>Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems</p>
E-safety Monitors	<ul style="list-style-type: none"> <li>● To uphold and promote the use of SMART rules and Top Tips to their peers</li> <li>● To provide useful information to other children in the school concerning online matters</li> <li>● To advise and comment on the following areas: Online Gaming,</li> <li>● Online Researching, Social Networking and Online Bullying on our VLE</li> <li>● To participate in e-Safety activities held by the e-Safety Coordinator</li> </ul>
Parent Support Workers	<ul style="list-style-type: none"> <li>● Educating Parents and raising awareness through coffee mornings and ongoing communication</li> <li>● Managing and reporting any parent concerns via CPOMs and offering 1:1 with the technician.</li> </ul>
Parents/carers	<ul style="list-style-type: none"> <li>● Consult with the school if they have any concerns about their children's and others' use of technology</li> <li>● Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.</li> <li>● Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns</li> <li>● Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.</li> </ul>

	<ul style="list-style-type: none"> <li>● If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the <a href="#">Online Tutors – Guidance for Parents and Carers</a> poster at <a href="http://parentsafe.lgfl.net">parentsafe.lgfl.net</a>, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online</li> <li>● Attend/engage in Online Safety workshops and events provided by the school.</li> </ul>
External groups	<ul style="list-style-type: none"> <li>● Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school</li> <li>● Support the school in promoting online safety and data protection</li> <li>● Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other’s images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers</li> </ul>
<p>Online Safety Team</p> <p>(Computing Lead, parent councillors, Parent Support Worker, ICT technician and Designated Safeguarding Lead)</p>	<ul style="list-style-type: none"> <li>● To meet termly to discuss any concerns parents might have.</li> <li>● For school to share new information and gain the best ways to share good online safety practice with the community.</li> <li>● To arrange training within the school community, where necessary.</li> </ul>