OLD PALACE & CHILDREN'S HOUSE FEDERATION

ONLINE SAFETY AND ACCEPTABLE USE POLICY

At the Federation, safeguarding and promoting the welfare of children is everyone's responsibility. The federation recognises that safeguarding incidents and behaviours can happen online as well as offline and that children can be vulnerable to a range of online harms. The policy sets out how the federation fulfils its statutory duty under the Keeping Children Safe in Education 2025, and sits alongside the federations Child Protection Policy. The policy ensures how the pupils are taught how to stay safe online and how to report concerns.

Online safety is an integral part of the federation safeguarding arrangements and is embedded within the whole federation approach to safeguarding.

The Federation acknowledges that:

- Children can be at risk of abuse or exploitation online
- Online abuse may be perpetrated by children or adults
- Online behaviour can be linked to wider safeguarding concerns

All online safety concerns are treated as **safeguarding concerns** and are managed in line with the Federation's Child Protection and Safeguarding Policy.

Aims

- Set out expectations for all Federation 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 inside and outside of the educational setting, 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 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 federation, supporting the ethos, aims and objectives, and protecting the reputation of the federation 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 Federation policies such as Behaviour Policy, Anti-Bullying Policy, Remote Learning Policy)

Why is internet use important?

The purpose of internet use in the federation is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the Federation'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 federation 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 community?

These can be summarised as:

The 4 key categories of risk Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, fake news (disinformation), deep fakes, conspiracy theories, racism, self-harm, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, over sharing personal data.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Who is responsible for Online Safety?

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

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

It is vital that all staff recognise that online safety is part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern.

Educating parents about Online Safety

The Federation raise parents/carers awareness of internet safety in newsletters or information via the Federation website, workshops, Parent Council meetings. If parents/carers have any queries or concerns in relation to online safety, these are addressed in the first instance by the Year Group Lead (or DSL) at Old Palace and with the Head of School at Children's House. If they require support setting up safety features on their devices, they can book an appointment with the ICT technician via the Parent Support Workers at Old Palace or Children's House office. Appointments will take place half termly.

How are pupils taught about safety online?

The federation has a clear, progressive Online Safety education programme as part of the Early Years PSED curriculum Computing and PSHCE curriculum. 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; including misinformation and fake news (disinformation).
- 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 (including the use of AI) 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 consent 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.

Digital Ambassadors

The Federation have digital ambassadors' from Year 5 and 6 at Old Palace who help raise and improve the profile and understanding of online safety across the community. They help promote online safety and provide information to other children and parents. By doing this, they ensure that children respect each other online and learn to make the right choices.

How are IT systems managed to support Online Safety?

Authorised Internet Access

- The Federation 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 Federation ICT resource (see appendix B)
- All pupils sign an Acceptable Use Agreement, agreeing to follow the Federation'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 Federations Acceptable Use Policy on the homepage
- The Federation is vigilant in its supervision of pupils' internet use at all times, as far as is reasonable, and uses age appropriate learning resources where older pupils have more flexible access;
- Parent/carers consent to pupils accessing the internet as part of the Home Federation Agreement (see Appendix E).

Appropriate Filtering and Monitoring

- The DSL and ICT technician will review the filtering and monitoring provision at least annually.
- All staff are aware of the filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking.
- Staff can submit any concerns by emailing the DSL and ICT technician.

- Half-termly checks take place to ensure the filtering is operational, functioning as expected.
- The Senso monitoring system is in place.

- Ensures staff read and sign that they have understood the Federation's Acceptable Use Policy. Following this, they are set up with Internet, google drive 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 on the iPads.
- 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, safe connection that is protected with firewalls and multiple layers of security, including a web filtering systemhttps://amifiltering.co.uk/.
- 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 the following child-friendly search engines where more open Internet searching is required: https://swiggle.org.uk/ https://www.kiddle.co/
- 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 Federation 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 educational settings.
- 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 or microsoft (password protected)
- 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 DSL. 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 Federation ICT systems regularly with regard to security.

Email

Staff and governors at the Federation use the StaffMail system for all work emails. This system is linked to the USO authentication system and is 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, Executive Headteacher/Head of School (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, Egress systems and microsoft (password protected) are available
    - ○ Internally, staff should use the Federation network, including when working from home when remote access is available via Google drive.
- 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 Federation 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 or after school/nursery and during designated breaks, providing pupils are not in the room

- ***Google email and google chat has been deactivated for pupils and staff. However, if there is activation this needs to be reported to the DSL.***

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. Federation staff will ensure that in private use:
    - ○ They do not engage in online discussion on personal matters relating to members of the Federation community. This includes making reference to pupils, parents and staff on social media
    - ○ Personal opinions should not be attributed to the Federation 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.

Federation Social Media Account

- The federation social media accounts are monitored daily to ensure comments and tags are appropriate and accurately reflect the setting.
- Notifications are enabled on the accounts so that staff monitoring the account are aware of the activity on the account to ensure it is in line with Federation's policy.
- Inappropriate comments or tags will be removed immediately and users will be blocked from seeing the account.
- The federation has a record of consent by the parents/carers for pupils who are allowed to be shown on the 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 accounts.

- Teachers may share the 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 state users must be over 13 years old to sign up for an account, we will not promote and will advise parents/carers to not allow their use by pupils at the Federation.

Social Media Incidents

- Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents is the Acceptable Use Policy.
- Breaches will be dealt with in line with the behaviour policy (for pupils) and Code of Conduct (for staff).
- Where an incident relates to an inappropriate, upsetting or abusive social media post by a member of the community, the Federation will request the post be deleted and will expect this to be actioned promptly. Failure to do so may impede the investigation of a complaint. The Federation may also report it to the platform it is hosted on and contact the Professionals' Online Safety Helpline (POSH) for support to accelerate the process.

Digital Images & Videos

- Videos and photographs of children and adults from the federation are included on our website, social media page and in the Federation 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 Federation 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 Federation 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 Federation website social media page (with parental consent)
- Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of safeguarding.

Use of Generative AI

At the federation, we acknowledge that generative AI platforms, such as ChatGPT, Gemini, Co Pilot or Adobe Firefly are becoming widespread.

We are aware that there will be use of these apps and exposure to AI creations on devices at home pupils.

The federation helps pupils to understand that not everything they see or hear online is "real" or unbiased, by blending smart technology with a curriculum of critical thinking and responsible use.

Cloud Environments

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

Federation and school/nursery Websites

- The Executive Headteacher takes overall responsibility to ensure that the websites content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our authorised website administrators
- The websites comply with the statutory DfE guidelines for publications;
- Most material is the Federation'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 Federation address, telephone number and we use a general email contact address, e.g. admin@oldpalace.towerhamlets.sch.uk for Federation Primary and admin@childrenshouse.towerhamlets.sch.uk for Children's House . Home information or individual email identities will not be published or shared.

Federation 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 Federation 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 Federation's policy on the use of personal mobile phones and devices?

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 Federation community (pupils, staff and visitors) while they are at Federation or undertaking Federation activities off site.

To note: devices refers to (but not limited to)- tablets, Smart watches and glasses (electronic wearables) etc.

General issues

- Mobile phones brought into Federation are entirely at the staff member, parents' or visitors' own risk. The Federation accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Staff and all visitors to the Federation 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 mobile phones and vice versa.
- Devices may only be added to the Federation wireless connection when being used for work purposes
- The Federation reserves the right to search the content of any mobile or handheld devices on the Federation 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 Federation site. These include: toilets, areas where pupils are changing for PE.

Staff

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal Federation 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 Executive Headteacher or Head of School. They should not be used in an area when pupils are 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. However, If personal equipment is being used for this purpose, for example during a residential visit, the number should be withheld and the Executive Head or Head of School informed. Personal numbers should not be shared with children or parents.
- Personal mobile devices should never automatically synchronise with any Federation endorsed system (except email), particularly where images from personal devices can be uploaded to Federation 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 Federation on the undertaking that the photographs are only used for approved Federation business and will be transferred to the Federation network as soon as practically possible, and will not be stored at home or on memory sticks.
- If videos or images are taken for Federation purposes they should be transferred to the Federation network at the end of the day and then be permanently deleted from the device
- Staff members can use a personal mobile phone during Federation visits in the event of an emergency to contact the Federation office or the emergency services.
- If a member of staff breaches the Federation 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 Federation 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 Federation website so this can be shared with families.

How does the Federation handle Online Safety Concern or Complaints?

Federation 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
- Information Governance Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

- All concerns are reported via CPOMS (cause for concern, Online) to the DSL without delay
- Action is taken and recorded to protect the child and prevent further harm
- Parents are informed where appropriate and advised.
- External agencies are involved- when required.

Any concern/allegation about staff misuse is always referred directly to the Executive Headteacher or Head of School, unless the concern is about the Executive Headteacher or Head of School in which case the complaint is referred to the Chair of Governors 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 DSL 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 Federation 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 Federation 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 Federation's 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 Executive 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 Federation (Appendix F)

- Pupils will be taught online safety through the Early Years PSED curriculum and 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)
- As part of the half termly safety assemblies, Online will be addressed.

Parents

- Online safety, access to the internet and use of digital images are discussed with parents at their child's admission interview
- The Federation website and newsletters remind parents of the importance of online safety.
- Parent workshops are provided throughout the year.
- Concerns discussed and shared in the Parent Council Meetings.
- 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.thinkyouknow.co.uk/parents

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

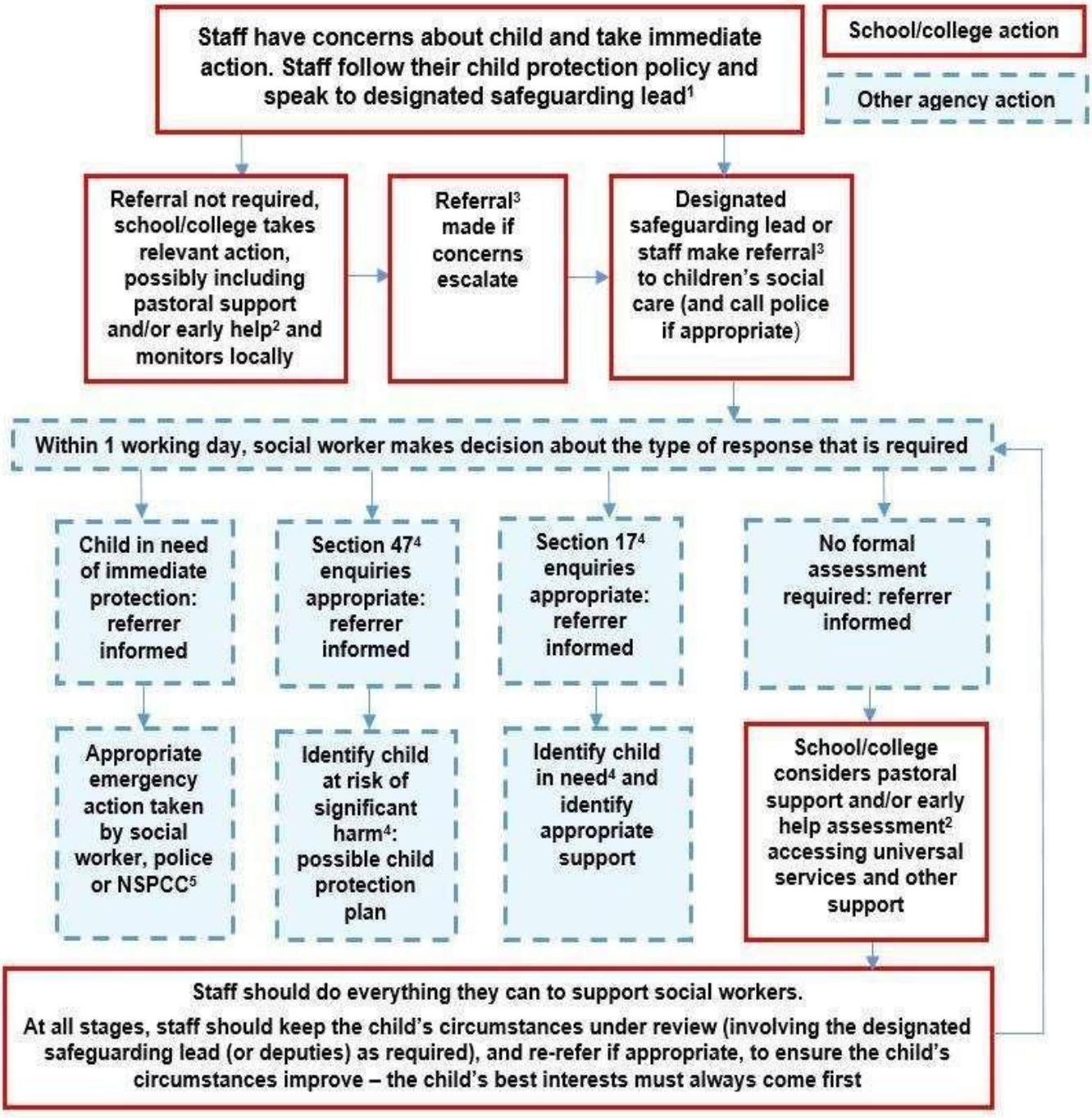
Childnet: http://www.childnet.com/sns

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


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Appendix B

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

1. Professional Conduct & Personal Responsibility

- I understand all information systems (email, internet, cloud storage) must be used primarily for professional purposes related to the school/organization.
- I will ensure that any communication sent via official channels is professional in tone and content.
- I will comply with the requirements under the heading- '**What is the Federation's policy on the use of personal mobile phones and devices?'**

2. Data Protection & Security

- I will not share Credentials and use complex passwords and, where available, Multi-Factor Authentication (MFA).
- When handling Sensitive information (student records, data etc.), they must only be stored on approved, encrypted platforms. I will not use personal cloud storage (e.g., personal Dropbox) for work-related sensitive data.
- I understand portable devices (laptops, tablets) must be locked when left unattended and should be kept in a secure location when off-site.

3. Social Media & Online Presence

- I must not "friend" or follow current students/parents on personal social media accounts.
- I will not post content that could bring the federation into disrepute.
- I will regularly check the security of my personal social media profiles.

4. Digital Safety & Safeguarding

- If there is accidental access to inappropriate content or discovery of a security breach must be reported to the ICT technician immediately (or DSL if not available).
- I will use official platforms for all communication with students/parents.
- **I** must not attempt to bypass web filtering or security software (e.g., via VPNs).
- I will ensure my personal devices/log-ins are not in sync with federation devices.

Remote & Home Working

- When accessing sensitive data offsite, I will ensure the screen is not visible to family members or the public.
- I will ensure Work-related paper documents and hardware must be stored securely when not in use.
- I will not leave "logged-in" devices unattended.

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 Federation's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Date: _____

Appendix C

KS1 Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...

I will only use a computer when an adult tells me I can.

I will keep my password safe and not share it with anyone.

I will always send polite messages.

I will tell an adult if I see something on the computer that makes me unhappy.

Inside school, my trusted adults are_____

Outside school, my trusted adults are_____

Signed: _____ **Date:** _____

KS2 Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe on the computer...

I will ask permission before using the Internet and use it for a specific purpose.

I will never share my personal details, such as my full name or address, with people I don't know.

I will never share my password with anyone.

I will never meet up with someone I have met on the Internet.

I will always check my messages are polite before I send them.

I will not reply to a message that isn't kind, but I will save it and show it to an adult.

I will not open or download a file unless I am sure it is safe.

I know I should not believe everything I read on the Internet.

I will always tell an adult if something on the Internet makes me or my friends unhappy.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

at school that might mean _____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed: _____ **Date: _____**

Appendix D

Acceptable Use Policy (AUP) for Parents

Objective: To ensure that all members of our school community use digital technology and social media in a way that protects the safety, well-being, and reputation of our pupils and staff.

Images and Media

1. Images taken at school events (plays, sports days) are for personal use only.
2. I will not post photos or videos on social media that include other children without the express consent of their parents.
3. I will not record or stream live during school performances, as it is prohibited to protect safeguarding protocols.

Social Media & Online Conduct

- I will refrain from making defamatory, offensive, or derogatory comments regarding the school, its staff, or pupils.
- If I have a grievance, I will use the school's official Complaints Procedure rather than airing concerns on public forums or class WhatsApp groups.
- I understand that online comments can be permanent and may cause distress to members of the school community.

Online Safety & Home Support

- I will model positive digital citizenship for my child.
- I will help my child stay safe by monitoring their internet usage at home and ensuring they only access age-appropriate content and platforms.
- If I become aware of any online bullying or inappropriate digital behaviour involving pupils, I will report it to the school

Communication with Staff

- I will use the official federation email addresses or office telephones numbers.
- I understand that staff/federation may not respond to digital communications outside of working hours.

By sending your child to the Federation, you agree to uphold these standards to help us create a safe "digital footprint" for all our students.

I/we have read, understood and agreed to this policy.
Signature/s: _____

Name/s of parent / carer: _____

Appendix E

Federation Internet Access and Use of Children's Work and Images

Parent's Consent for Internet Access

At the Federation we believe that the Internet is an essential part of your child's learning. The Federation 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 Federation website should you require more details.

- **I give permission for my child to have access to the internet and agree that the Federation is not liable for any damages arising from use of the internet facilities.**
- **I understand that the Federation will take all reasonable precautions to ensure pupils cannot access inappropriate materials and that the Federation 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 Federation displays and celebrations of the pupils' work, on our Federation website, social media account and on documents relating to the school, for example our Federation 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 Federation assemblies, trips and other supervised Federation activities. Video recording is not permitted.

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

	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 Federation 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	

Signed by parent/carer	**Date:**
Name of child:	**Class:**

Appendix F

e-Safety SMART Rules

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

s SAFE	Keep SAFE by asking permission before using the internet, going onto any website or opening unknown files/emails. Do not give out personal information such as your phone number, your real name, your school name or password to anyone online.
m MEETING	MEETING someone from the internet can be dangerous. Only do so with your parents' or carers' permission and only when they are there with you.
a ACCEPTING	ACCEPTING 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!
r RELIABLE	Think 'How RELIABLE is it?' Some information on the internet may not be true. People you meet online may lie about themselves.
t TELL	TELL 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.

e-Safety Top Tips

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

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

Appendix G

Federation iPad Loan Agreement Staff

iPad Make/Model	
iPad Serial Number	

This agreement is between:

OPCH Federation

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 Federation and is governed by their policies.

- The Federation is lending the Staff an iPad for the purpose of doing work.
- This agreement sets the conditions for taking an iPad 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/Stolen

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, faults, defects, lost or stolen, I will immediately inform the Federation.
- If the equipment is stolen, I will also immediately inform the police, as well as the Federation.
- I agree to keep the equipment in good condition and to return it to the Federation on their demand, in the same condition.
- I will not leave the equipment unsupervised in unsecured areas.

Where damage to school equipment is found to have occurred as a result of neglect, misuse, inappropriate handling or a failure to follow agreed procedures or training, the school will be required to investigate the matter. In such circumstances, this may be managed through the school's disciplinary process, in line with the Disciplinary Policy.

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.

- Federation 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 Executive Headteacher or Head of S
- 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 Federation's Volume Purchasing Programme. If a class set is required, a request will need to be sent to the ICT Technician. 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 Federation Agreement for new arrivals.
- Any photographs taken of pupils should be transferred to the Federation network and then deleted by the end of the 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.

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 Federation 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.

Return date

I will return the device and accompanying charger in its original condition and box to the Federation 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.

DATE	
STAFF MEMBER NAME	
STAFF MEMBER SIGNATURE	
DATE	
DATE RETURNED	
DEVICE CHECKED BY	

Appendix H

Governing Body

- Safeguarding policies, including online safety, comply with statutory guidance
- Appropriate filtering and monitoring systems are in place
- The effectiveness of safeguarding arrangements is regularly reviewed

Executive Headteacher and Head of School

- Has overall responsibility for safeguarding and online safety
- Ensures staff receive appropriate training and updates

Designated Safeguarding Lead (DSL)

- Takes lead responsibility for safeguarding, including online safety
- Is appropriately trained and supported
- Acts as a point of contact for online safety concerns
- Refers cases to external agencies where necessary

Staff

- Understand that safeguarding is everyone’s responsibility
- Are aware of the systems in place for reporting concerns
- Are alert to signs that a child may be at risk online
- Report concerns immediately to the DSL