The Park Federation
ACADEMY TRUST

Online Safety Policy
2026-27

Approved by	Helen Abell, CEO		
Date	August 2026	**Next review due**	August 2027

Summary of Changes

Version	Date	Summary of Changes	Approved By
1	August 2024	Updated to be in line with KCSIE 2024	CEO, on behalf of the Board of Directors
2	August 2025	-Added a version history table. -Updated to be in line with changes to KCSIE 2025. -Included the use of Senso as an additional monitoring system -Introduction of information around the use of Artificial Intelligence (AI).	CEO, on behalf of the Board of Directors
3	August 2026	Updated throughout to be in line with changes to KCSIE 2026. -Updated key staff and designations throughout the policy. -Added new guidance materials and updated weblinks in accordance to KCSIE 2026. -In roles and responsibilities, re-phrased what to do when recording online incidents for children and for cases of network, filtering and monitoring incidents for better clarity. - In Section 3, CH has added 3.8-3.11 to provide information on other roles in the school who have a responsibility for online safety. - 3.13 – Added a link to the National College for parents and carers - 3.14 & Section 15 – Added information on the use of mobile phones in school - Added Mobile Phone Policy to the linked policies list. - On Section 5 – Safe use of social media and the internet reworded and updated. - Section 7 – Clarified reporting procedures for sexual abuse and the discovery of nudes and semi nudes - Section 9 – Updated information on child on child abuse - Section 19 – Now information on Data Protection and Cyber Security - Updated contents and appendices in line with changes made	CEO, on behalf of the Board of Directors

Contents

Heading	Page
1. Aims	4
2. Legislation and guidance	4
3. Roles and responsibilities	5
4. Use of technology in the classroom	12
5. Educating children about online safety	13
6. Educating parents and carers about online safety	14
7. Managing online safety	15
8. Cyber-bullying	16
9. Child on child sexual abuse, harmful sexual behaviour, sexual harrasment and sexual violence	18
10. Grooming and exploitation	19
11. Mental Health	20
12. Online hoaxes and harmful online challenges	20
13. Cyber-crime	21
14. Acceptable use of the internet in the academy	22
15. The use of mobile phones in the academy	22
16. Staff using devices outside of the academy	23
17. Remote Learning and the Federation Digital Strategy	24
18. How the academy will respond to issues of misuse	24
19. Data protection and cybersecurity	25
20. Training	25
21. Monitoring arrangements	26
22. Links with other policies and legislation	27
Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers)	27
Appendix 2: KS2 acceptable use agreement (children and parents/carers)	29
Appendix 3: Acceptable use agreement (staff, trainee teachers, Academy Council members, Board Directors, volunteers and visitors)	31
Appendix 4: Online safety training needs – self-audit for staff	32
Appendix 5: Online safety incident report log	33

Appendix 6: Flowchart for reporting concerns around online safety	34
Appendix 7: Staff handout of the Federations Approach to Filtering and Monitoring	36

1. Aims

The Park Federation Academy Trust (TPFAT) and its academies aim to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and Academy Council (AC) members and Board of Directors (BoD)
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer 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, including those generated using AI and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If the school feels the pupils or staff are at risk, please report it to **Chris Newton – TPFAT Network Manager**. You can also report to the Anti-Phishing Working Group (https://apwg.org/).

2. Legislation and guidance

This policy is written in line with the following:

- Department for Education's statutory guidance, **Keeping children safe in education 2026**, which comes into force on 1st September 2026.
- DFE's Filtering and Monitoring Standards (paragragh 142) which now has reference to the departments 'Plan Technology for your School' service
- DFE Genrative AI: Product Safety Expectations - for information on how to use generative AI safely and how filtering and monitoring requirements apply to the use of generative AI in education
- DfE's Mobile Phones in School (2026)
- DfE's filtering and monitoring standards
- Education for a Connected World and Meeting Digital and Technology Standards in Schools and Colleges, and its advice for schools on:
  - Teaching online safety in schools
  - Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
  - Relationships and Sex Education
  - Searching, screening and confiscation
  - It also refers to the DfE's guidance on protecting children from radicalisation and Statutory guidance on the Prevent duty (2023).

It reflects existing legislation, including but not limited to the below:

- Online Safety Act (2023), a new set of laws that protect children and adults online.
- Education Act 1996 (as amended)
- the Education and Inspections Act 2006
- Equality Act 2010.

- In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber- bullying by, if necessary, searching for and deleting inappropriate images or files on children' electronic devices where they believe there is a 'good reason' to do so.
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 DfE (2021) 'Harmful online challenges and online hoaxes'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi- nudes: advice for education settings working with children and young people'

- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

3. Roles and responsibilities

3.1 Board Directors

Board Directors have overall responsibility for monitoring this policy and holding the CEO and Principal to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Academy Council will co-ordinate regular meetings with appropriate staff to discuss online safety, and
monitor online safety logs as provided by the designated safeguarding lead (DSL) on behalf of the Board Directors.

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

The Academy council member who oversees online safety is **Sam Eversden**

The Board Director with a focus on online safety **is Ranisha Dhamu**

The Online Safety Leads at Iver Village Infant Academy is **Corina Constantinescu**

The Director of Digital Learning at The Park Federation Academy Trust, and Digital Lead at JEA, is **Carolyn Hillarious**

TPFAT Network Manager is **Chris Newton**

The Academy SENDCo is **Kate Sibley**

Board Directors and Academy council members will:

- ensure that they have read and understand this policy
- agree and adhere to the terms on acceptable use of the academy's IT systems and the internet (appendix 3)
- ensure that online safety is a running and interrelated theme while devising and implementing their whole trust wide academy approach to safeguarding and related policies and/or procedures
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some children with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- ensure the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness.
- ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.
- Ensure that the designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place), which should be explicit in the role holder's job description.

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

3.3 The Designated Safeguarding Lead

Details of the designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our child protection and safeguarding policy as well as relevant job descriptions. The Designated Safeguarding Lead at is **Rebecca Pinkney (Vice Principal)**, the Deputies are **Tajinder Johal (Principal), Jasvir Chander (Vice Principal) and Vanda Devshi (Vice Principal).**

The DSL takes lead responsibility for online safety, including an understanding of filtering and monitoring, in the academy, in particular:

- Acting as the named point of contact, alongside the Online Safety Leads, within the academy on all online safeguarding issues.
- Ensuring appropriate referrals are made to external agencies, as required.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that children with SEND face online.
- Showing an understanding of the filtering and monitoring systems and processes in place.
- Ensure that training for staff, including those at induction, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.
- Ensuring online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Working with the Principal, IT Network Manager, SENDCo and online safety lead, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the academy Child Protection and Safeguarding Policy JEA Child Protection and Safeguarding Policy, with support

from the Online Safety Leads.

- Ensuring that any online safety incidents involving pupils are logged on CPOMs and any networking, monitoring or filtering incidents are reported to the Network Manager, (see appendix 5 for an example of a recording sheet if required) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged in CPOMs and dealt with appropriately in line with the academy's Positive Behaviour Policy.
- Updating and delivering staff training on online safety, which includes information about filtering and monitoring. See appendix 4 which shows an example of a self-audit for staff on online safety training needs.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety to the Academy Council
- Ensuring safeguarding is considered in the whole academy approach to remote learning.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating, alongside the Digital Lead and Online Safety Lead, the academy's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by children and staff.
- Ensuring all members of the school community understand the reporting procedures.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the academy's provision, and using this data to update the academy's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Meeting with the Network Manager termly (DSL Hub Leads) to review web filtering systems including reviewing blocked and unblocked categories and to disseminate this information to other DSLs within each hub.
- Working with the Principal and Online Safety Leads, Lead for Digital Learning and Network Manager to conduct half-termly light-touch reviews of this policy.
- Work in collaboration with the Digital Lead and the Online Safety Lead to review the academy's 360 Online Safety Review Toolkit annually.

This list is not intended to be exhaustive.

3.4 The IT Network Manager

The IT Network Manager is **Chris Newton.**

They are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children are kept safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material. Throughout the The Park Federation Academy Trust, this is **through LGfL Webscreen, Youtube Strict, Google Safe Search and Senso (a monitoring system used to alert staff to any potential online safety concerns).**
- Ensuring that the IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Working with London Grid For Learning (LGFL) and Class Technology, conducting a full security check and monitoring the trusts IT systems on a weekly/fortnightly/monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5 for an example) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are escalated to the Senior Leadership Team and dealt with appropriately in line with the academy Positive Behaviour Policy

- Attending termly meetings with the Chief Executive Officer (CEO), Safeguarding representative from the Board of Directors, DSL Hub Leads for Slough and Hillingdon schools, and the Director for Digital Learning to monitor and discuss web filtering (what's blocked, what's not and why)

- Providing technical support in the development and implementation of the Trusts online safety policies and procedures.

This list is not intended to be exhaustive.

3.5 The Digital Lead

The Director of Digital Learning and the Digital Leads are responsible for:

- Staying informed on best practices about using technology safely for teaching and learning
- Supporting the school's DSL and other digital leaders in implementing best practices for online safety in schools.
- Supporting teachers with resources and teaching materials that explicitly teach online safety behaviours
- Creating or Co-Creating with the school Senior Leadership team, policies or contracts for the safe and appropriate use of technology in schools.
- Supporting parents and the wider school community by disseminating online safety information to support the safe use of technology at home and in school.
- Supporting schools in monitoring online safety environments by conducting audits and providing the next steps for improvement.
- Work with the school IT department to ensure the smooth running of systems and policies in place for safe use
- Support the IT department with monitoring the GDPR requirements for external apps, extensions and programs to ensure compliance requirements are being met.

This list is not intended to be exhaustive. Please see the Digital Strategy Policy (link needed) for further information.

3.6 The Online Safety Lead

The Online Safety Lead is responsible for:

- Promoting a culture of online safety within the school by using and sharing a variety of resources (e.g online safety calendar, anti bullying week and Safer Internet Day resources) to raise awareness throughout the academic year
- Liaising with the DSL/DDSLs in reviewing and updating the Online Safety Policy and the school's procedures to managing and responding to online safety concerns, at least annually
- Liaise with the curriculum teams to ensure online safety is embedded throughout the curriculum
- Working with the DSL/DDSLs in response to online safety breaches and concerns to support further education for individuals, groups, classes or year groups as deemed necessary
- Working with the DSL to look at patterns and trends in online safety concerns and work towards solutions to reduce these incidents

- Undertaking own online safety CPD and contributing to the online safety CPD of all staff to keep knowledge and understanding fresh and up to date.

- Contributing to the annual online safety audit alongside other relevant staff, such as the DSL, Digital Lead, Safeguarding Governor
- Being aware of the school's web filtering systems that reduce the risk of online harms
- Sharing information on online safety to children, parents and carers
- Lead or contribute to the annual online safety audit
- Prepare supporting evidence and liaise with Digital Lead for the Federation Digital Review Day

This list is not intended to be exhaustive. Please see the Digital Strategy Policy (link needed) for further information

3.7 All staff and volunteers

All staff, including trainee teachers, contractors, agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and maintaining a professional level of conduct in their personal use of technology.
- Implementing this policy consistently and modelling good online behaviours.
- Agreeing and adhering to the terms on acceptable use of the academy's IT systems and the internet (appendix 3), and ensuring that children follow the terms on acceptable use (appendices 1 and 2)
- Having an awareness of online safety issues, including how the school reduces the online harms to children through the use of appropriate web filtering through LGfL Web Screen, Safe Search, YouTube Strict and Senso.
- Working with the DSL to ensure that any online safety incidents are reported and logged on CPOMs for concerns about children, or with the Network Manager for incidents involving the network, filtering or monitoring systems and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately and recorded on CPOMs in line with the **Positive Behaviour Policy** and the **Child Protection and Safeguarding Policy**

3.8 Governing Body, led by Online Safety / Safeguarding Link Governor – Sandra Hopkins

Key responsibilities (guidance taken from Keeping Children Safe in Education)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board .
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated –
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated annually.
- The online safety governor should work closely with the DSL on the new filtering and monitoring standards.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Governing bodies should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness at least once every academic year .
- Read all of KCSIE to ensure all governors understand their safeguarding responsibilities.
- Work with the DPO, DSL and Principal to ensure a compliant framework for storing data,

helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.

- Ensure all school staff have read Part 1 of KCSIE – governors are recommended to read ALL of KCSIE to ensure they fully understand their safeguarding responsibilities.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Ensuring they are familiar with, and understand, the indicators that children may be unsafe online.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Engaging in training around online safety, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

This list is not intended to be exhaustive.

3.9 PSHE / RSHE Lead/s – Priyanka Gulati and Arlinda Osbaldeston

- As listed in the 'all staff' section, plus:
- Embed statutory RSHE Guidance, including consent, mental wellbeing, healthy relationships and staying safe online, as well as raising awareness of the risks and challenges from the latest trends in generative artificial intelligence (including deepfakes and digitally altered imagery), financial extortion and making/sharing nudes and semi nudes pictures online and misogynistic influencers, into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. It will also include recognising when they have experienced any online harm and who to speak to for support. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools, in an age-appropriate way to help pupils navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" –to complement the computing curriculum.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within PSHE / RSHE.
- Develop and implement a RSHE policy and publish this on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

3.10 Computing Lead – Gulnaz Azram

As listed in the 'all staff' section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL and all other staff to ensure understanding of the issues, approaches, and messaging within Computing.
- 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.

3.11 Subject leaders

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the PSHE/RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework 'Education for a Connected World' and 'Teaching Online Safety in Schools' can be applied in your context.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject-specific action plans also have an online safety element.

3.12 Children

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents, including those involving problems with filtering and monitoring, and concerns in line with the procedures within this policy.
- Are aware of Senso and how it alerts staff to any potential online harm.

3.13 Parents/carers

- Parents/carers are expected to:
- Notify the DSL/DDSL or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's IT systems and internet (appendices 1 and 2)
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- The National College – National Online Safety learning platform

3.14 Visitors and members of the community

Visitors and members of the community who use the academy's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Visitors and members of the community will also be expected to follow the school's mobile phone policy. This policy sets out the school's approach to mobile phones and other smart technology. The aim is to establish a calm, safe and supportive environment conducive to teaching by ensuring the school is a mobile free environment by default. Anything other than this should be by exception only. Please read the school's Mobile Phone Policy for more detailed information.

4 Use of technology in the classroom

James Elliman Academy utilises a range of technology to enhance learning, ensuring all use is safe and purposeful.

4.1 Review and Supervision

Prior to using any websites, tools, apps, or other online platforms in the classroom, or recommending them for home use, the class teacher will always review and evaluate the resource for appropriateness and safety. Children will be actively supervised when using online materials during lesson time, with supervision suitable to their age and ability. Class teachers will also ensure that any internet-derived materials are used in line with copyright law.

4.2 Filtering and Monitoring

All internet use on school Chromebooks and other school IT systems goes through the school's safety filters to ensure content is safe for children. We monitor all internet traffic to block harmful and inappropriate content. This includes the use of monitoring software like **Senso**, which helps spot worrying online behaviour on devices. The effectiveness of these provisions will be reviewed at least annually to meet safeguarding needs, as required by Keeping children safe in education 2026.

4.3 Generative Artificial Intelligence (AI)

In line with government guidance and our school AI policy, pupils will not be directly exposed to or interact with generative AI tools. Teachers may use AI tools to help them prepare lesson materials, but this will always be thoroughly checked by the teacher to ensure correctness and appropriateness. While pupils will not directly use these AI tools, some of our educational programs may utilise a type of AI that helps provide personalised support to pupils as they learn.

Our school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to generate or digitally alter images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. We will treat any use of AI to bully pupils very seriously, in line with our anti-bullying, child protection and safeguarding and positive behaviour policies.

Visual clues to look out for when suspecting AI generated harmful content
Images and videos:

- Unnatural features – Look for odd proportions, unusual lighting, or distorted backgrounds
- Hands and fingers – AI often struggles with these; check for extra fingers, missing digits, or strange positioning
- Facial inconsistencies – Mismatched earrings, asymmetrical features, or unnatural skin textures
- Text and logos – Garbled or misspelled text within images

- Lighting and shadows – Shadows that don't match the light source or seem inconsistent

What to Do When You Discover AI generated harmful content / Nude or Semi-Nude Images
DO NOT:

- Take a screenshot
- Forward or share the image
- Print the image
- Save or download the image
- View the image any more than is necessary to identify what it is

DO:
Confiscate the device (if appropriate and safe to do so)

- Turn off the device and secure it
- Do not search through the device

Record the details immediately by writing down**:**

- The date and time you became aware of the image
- Who reported it or how you discovered it
- What device it was on (e.g., "pupil's iPhone", "school iPad")
- A brief description of what you saw (without viewing it again)
- Any relevant context (e.g., "pupil reported receiving unsolicited image via Snapchat")
- Who else knows about it

Report to the DSL/DDSL immediately

- Do not delay
- Pass on the written information and the device (if confiscated)
- The DSL/DDSL will decide next steps, which may include contacting police

Preserve the device

- Keep the device secure and switched off
- Do not allow anyone else to access it
- Hand it to the DSL or police as directed

5 Educating children about online safety

James Elliman Academy will equip children and young people with the knowledge, understanding, and skills to navigate the digital world safely and responsibly. Our online safety education will be delivered across the entire curriculum and as part of a whole-school approach.

This education is underpinned by the National Curriculum computing programmes of study and the Department for Education's statutory guidance on relationships education, relationships and sex education (RSE), and health education, which all schools and academies will teach in primary settings.

We will integrate the themes and learning outcomes from the UK Council for Internet Safety (UKCIS) 'Education for a Connected World - 2020 edition' framework. This comprehensive framework, alongside the National Curriculum and RSE guidance, will ensure pupils develop understanding across key aspects of online education, tailored to their age and stage:

All schools and academies have to teach:

- Relationships education and health education in primary settings. This is set out in the DfE's statutory guidance.

In **Key Stage 1**, children will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Children in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns

about content and contact

- Think carefully about whether online information is true, reliable and safe before trusting it. This means checking where information comes from and understanding that not everything online is real.

By the **end of primary school**, children will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects and assemblies where relevant.
We utilise data from our safeguarding reports, filtering logs, monitoring captures, parental complaints and other stakeholder feedback to inform our curriculum, so that we are constantly learning from concerns and being reflexive and responsive to the needs of our children.
We recognise that nationally, children with SEND are less likely to receive effective online safety teaching, but are more at risk of being a victim of harm caused online. Therefore, we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children need to protect them from harm and prevent future online harm.

6 Educating parents/carers about online safety

The academy will raise parents'/carers' awareness of internet safety in letters, via the academy app and the academy website. This policy will be shared with parents/carers via the academy website.

The academy, through this policy, have let parents/carers know through this section:

- That we partner with London Grid for Learning for website filtering and monitor online use

Where the academy holds parent evenings we will cover:

- What their children are being asked to do online, including the sites they will be asked to access and who from the academy (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL/DDSL.

Concerns or queries about this policy can be raised with the DSL/DDSLs or the Principal.

Parents/carers/carers can also sign up to National Online Safety, for free, for up-to-date information on staying safe online. Parents/carers should speak to the Online Safety Lead, or their child's class teacher, about gaining access to this, or by following the link in Section 3.13 page 11 of this policy.

7. Managing online safety

7.1 Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the academy's approach to online safety, with support from deputies and the Principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about children' safety online. This includes an understanding of the filtering and monitoring systems in place. The responsibilities of The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all academy operations in the following ways:

- Staff and Academy Council members receive regular training, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online

7.2 Handling online safety concerns

Any disclosures made by children to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

All cases of child sexual abuse, including the making and sharing of consensual and non-consensual nudes and semi nudes, must be immediately reported to the DSL or DDSL, both verbally and via CPOMs. Sexual abuse imagery may also include the use of deepfakes, AI generated or digitally altered images. This reporting is in line with the statutory duty under Keeping Children Safe in Education (KCSIE). The DSL or DDSL will then report any child sexual abuse to the local authority and, if necessary, the police as per school policy and KCSIE guidance.

Staff will be aware that children may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that children displaying this type of behaviour are often victims of

abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in

order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's
parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the
information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Principal, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff (within Child Protection and Safeguarding Policy), and Disciplinary Policy and Procedures. If the concern is about the Principal, it is reported to the Chief Executive Officer (CEO), Helen Abell. If the Concern is related to the CEO then the matter is referred to Board Director for Safeguarding, **Ranisha Dhamu**. The LADO will also be contacted for advice and guidance.

Concerns regarding a child's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Principal and IT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Positive Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Principal contacts the police.

The academy avoids unnecessarily criminalising children, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the academy's response are recorded on CPOMs.

8. Cyber-bullying

a. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (see our Child Protection and Safeguarding Policy and our Positive Behaviour Policy).

b. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE)

education, and other subjects where appropriate.

All staff, AC members, BoD and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training (see section 11 for more detail).

The academy also sends information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the positive behaviour policy. Where illegal, inappropriate or harmful material has been spread among children, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL/DDSLs will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

c. Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on children' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of our academy rules

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal and DSL.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/DDSLs or other member of the senior leadership team to decide whether they should:

i. Delete the material, or

ii. Retain it as evidence (of a possible criminal offence* or a breach of academy discipline), and/or

iii. Report it to the police**

Staff must understand that whilst the making and sharing of nudes and semi nudes involving children (created via AI or otherwise) is illegal, pupils should be[CH4] [RW5] [RW6] encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area.

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they **will not** view the image but will report this to the DSL/DDSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of children will be carried out in line with:

iv. The DfE's latest guidance on searching, screening and confiscation

v. UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on children' electronic devices will be dealt with through the complaints procedure.

The school will also make use of guidance from The Marie Collins Foundation with regards to supporting victims of
Technology Assisted Child Sexual Abuse.

9. Child-on-child sexual abuse,harmful sexual behaviour, sexual harrasment and sexual violence

Children may also use the internet and technology as a vehicle for sexual abuse and harassment. Harmful sexual behaviour exists on a continuum and may escalate into sexual harassment or sexual violence. Therefore, It is important that staff identify inappropriate behaviour and intervene early. Staff will understand that this abuse can occur both in and outside of the academy, off and online, and will remain aware that children are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Online sexual harassment - Sexualised online cyberbullying, e.g. sexual jokes or taunts unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual making and sharing of nudes and semi nudes (including AI-generated images)
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse
- Coercion or pressure online
- Online grooming
- Online exploitation

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to children becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the

child themselves.

The academy will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other children taking “sides”, often leading to repeat harassment. The academy responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the premises or using academy-owned equipment. Concerns regarding online child- on-child abuse are reported immediately to the DSL/DDSL both verbally, and on CPOMs. The DSL/DDSL will investigate the matter in line with the Child Protection and Safeguarding Policy, Positive Behaviour Policy, Anti-bullying Policy, Mobile Phone Policy and the Social Media Policy.

10. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that children who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The child believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact children are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL/DDSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the academy and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

The Centre of Expertise on Child Sexual Abuse have produced new resources to help education professionals identify and respond to concerns of child sexual abuse and abusive behaviours. There is also additional support for educational professionals from The Children’s Society and Home Office's guide to preventing child sexual exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these

crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about children with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation/PREVENT

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain children at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy and Prevent Risk Assessment. Staff will be expected to exercise vigilance towards any children displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL/DDSL without delay, who will handle the situation in line with the Prevent Duty Procedures, as outlined in the Child Protection and Safeguarding Policy.

The school's web filtering systems have a range of categories that are blocked so that searches, or content around extremist views, hate crime and serious violence are significantly reduced. An example of some of the blocked categories are: *extreme, violence, profanity, security threats, search keywords, weapons and bombs, hate speech, social networking, criminal skills.* The school is mindful not to over block content which could compromise a broad and balanced curriculum. To further reduce the risks of children coming in contact with radicalised and extremist views, as with any other wider safeguarding concern such as Child Sexual Exploitation (CSE) or Child Criminal Exploitation (CCE), staff ensure that children are supervised at all times when using computers and devices which have access to the internet. LGfL Webscreen, Google Safe Search, YouTube Strict and Senso also provide additional protection to wider safeguarding issues such as radicalisation, extremist views, CSE and CCE. Any visitors who are invited to conduct talks, presentations or workshops will have their content approved by the Senior Leadership Team prior to being allowed to present to children.

11. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in children, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of the academy can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Pupil Wellbeing Policy.

To support our students in managing their own well being we will actively teach the 'Health, wellbeing and lifestyle' strand from the UK Council for Internet Safety (UKCIS) 'Education for a Connected World' framework, emphasising healthy online habits and the balance between online and offline activities.

12. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst children in the academy, they will report this to the DSL/DDSL immediately.

The DSL /DDSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to children, and whether the risk is one that is localised to the academy or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL/DDSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL/DDSL and the Principal will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact- checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing children.
- Not inadvertently encouraging children to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger children but is almost exclusively being shared amongst older children.
- Proportional to the actual or perceived risk.
- Helpful to the children who are, or are perceived to be, at risk.
- Appropriate for the relevant children' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting children at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant children, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL/DDSL and Principal will only implement an academy-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing children' exposure to the risk is considered and mitigated as far as possible.

13. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber- crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with

internet traffic to render it unavailable.

The academy will factor into its approach to online safety the risk that children with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL/DDSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL/DDSL and Principal will ensure that children are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that children cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on academy-owned devices or on academy networks through the use of appropriate firewalls.

14. Acceptable use of the internet in the academy

All children, parents/carers, staff, volunteers and Academy Council members and Board of Directors are expected to sign an agreement regarding the acceptable use of the academy's IT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by children, staff and all other adults (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

15. The Use of Mobile Phones in the Academy

a. Children using mobile devices in the academy

Children in years 5 and 6 may bring mobile devices into the academy, if they are walking to and from the academy alone. Please see our **Safe Handover/Children Walking Home Alone Policy** for further information. Mobile phones are not permitted to be used during:

i. Lessons

ii. Break times and lunchtimes

iii. Clubs before or after school, or any other activities organised by the school

Children are expected to tell their teacher that they have their mobile phone with them and this should be turned off and handed into the school office on entry to school and collected at the end of the day. The school office will safely store all mobile phones until the end of the day. All phones must be clearly labeled with the child's name and class. Children are not allowed to use their mobile phone until they are out of the academy grounds.

Children are permitted to bring their mobile phone to school if it is used for medical purposes.

Any use of mobile devices in the academy by children must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a child may trigger disciplinary action in line with our positive behaviour policy, which may result in the confiscation of their device.

b. Staff using mobile devices in an Academy

Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Multi-Factor Authentication (MFA) is strictly enforced on all mobile devices accessing academy accounts and networks. Both remote access and access to school emails, platforms, and cloud services require MFA verification. Any device that is not compatible with MFA will not be permitted to access, connect, or link up to our cloud servers.

USB storage, downloading, and data transfer functionality is strictly disabled across all school computers and technical infrastructure. Personally-owned mobile devices, external drives, or hardware cannot be connected to school computers, laptops, or servers via USB for data transfer, file downloading, or charging.

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. Staff must not use their own mobile phones in children's toilets or changing rooms.

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth
communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by the Principal. Where a personal call is needed to be taken, this must be done out of the view of children.

Staff should not use 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 a member of staff breaches the academy policy then disciplinary action may be taken.

Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents/carers, then an academy mobile phone will be provided and used. In an emergency where a staff member doesn't have access to an academy-owned device, they should 'hide' their own mobile number for confidentiality purposes, using their Caller ID settings, or adding "141" before the number to be dialed.

It is at the discretion of the Principal whether whole staff group chats are used In schools for emergency communication purposes. If this is the case, staff must exercise the Staff Code of Conduct and behave professionally. No photographs of children are to be used during this communication.

For further information on the use of mobile phones in school please read the Mobile Phone Policy.

16. Staff using work devices outside of the Academy

All staff members must take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always install the latest updates
- Both remote access and access to school emails are two factor authenticated for added security.

Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the academy IT Network Manager.

17. Remote learning and the Federation Digital Strategy

All remote learning is delivered in line with the **Remote Learning Policy.**

The academy will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The academy will consult with parents/carers prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The academy will ensure that all academy-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the academy will maintain regular contact with parents/carers to:

- Reinforce the importance of children staying safe online.
- Ensure parents/carers are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents/carers to useful resources to help them keep their children safe online.
- Reinforce the importance of learning in a mobile free environment.

The academy will not be responsible for providing access to the internet off the academy premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the academy.

The Federation Digital Strategy

The Park Federation is building a one-to-one digital learning strategy in all or its ten schools with the vision of providing each of its pupils with a Chromebook as a digital learning tool to amplify and enhance learning. Technology will always be used as a tool to enhance the already good teaching and learning practices that are already in its academies. Technology will also be used as a vehicle to bring access and equity to all learners in our schools. At James Elliman Academy all pupils in Year 4, Year 5 and Year 6 use a Chromebook in school to support their learning and enabling teacher to extend the learning environment beyond the four walls of the classroom. Online Safety lessons are explicitly taught and interwoven into daily teaching using digital tools.

18. How the Academy will respond to issues of misuse

Where a child misuses IT systems or internet, we will follow the procedures set out in our policies on positive behaviour, and any other relevant Park Federation Policy linked to IT, social media or internet use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's IT systems or the internet, or misuses a

personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and any other relevant Park Federation Policy linked to IT, social media or internet use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

The academy will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device. Neither the academy nor The Park Federation Academy Trust can accept liability for material accessed, or any consequences of Internet access.

Staff and children are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher/ Year Leader/ Vice Principals/ online safety Lead/Designated Safeguarding Lead or Deputy Designated Safeguarding Lead/Principal;
- informing parents/carers or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.
- Referrals to outside agencies which can support the education of online safety

Complaints of cyberbullying are dealt with in accordance with our Positive Behaviour Policy and Anti-Bullying Policy.

Complaints relating to child protection are dealt with in accordance with child protection and safeguarding Policy.

The online safety Lead will keep a record of issues relating to pupil misuse of email or internet services and will liaise with the Safeguarding Team and the IT Network Manager as required.
Appendix 6 shows a simple flowchart of what to do if you discover an online safety breach.

19.Data Protection and Cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policies. (Please refer to the data protection policy).

It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE, which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

20. Training

All new staff members will receive training, as part of their induction, on safe internet use, the schools filtering and monitoring systems in place, as well as online safeguarding issues including cyber-bullying, cybersecurity and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all

contain an online element Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL/DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our **Child Protection and Safeguarding Policy**.

21. Monitoring arrangements

All staff can log behaviour and safeguarding issues related to online safety using CPOMs (categories Safeguarding and Welfare Concern Form and Serious Inappropriate Incident/cyber bullying/online safety). If CPOMs is not accessible staff will refer using the paper copy found on all year group's boards and in the office. An incident report log, for the most serious cases is used and can be found in appendix 5. The staff member will need to inform the Principal, DSL/DDSLs and the online safety lead as per usual safeguarding reporting procedures. The Principal, DSL/DDLSs and or the online safety Lead will alert the IT Network Manager immediately. Steps will then be taken to resolve the matter. Appendix 6 shows a flowchart of actions in the event of a complaint or online safety breach of any kind.

To further ensure effective online safety, James Elliman Academy will employ detailed monitoring practices:

Preventative Monitoring: We will ensure Google SafeSearch is turned ON and use comprehensive filters to block social media, games, and other unsuitable content across school Chromebooks and IT systems. Teachers will actively watch how students use devices in class and guide them to safe websites.

Responsive Monitoring: We will use monitoring software, such as Senso, to spot any worrying online behaviour on school devices. School staff will review this information to identify and respond to any risks or misbehaviour.

Technical and safeguarding colleagues work together closely to carry out an annual review and regular checks of filtering and monitoring, and to ensure that the school responds to issues, considers how to prevent further concerns and integrates with the curriculum.

Where staff use Generative AI, they must be pre-approved by the school. For children and young people, we block the generative AI category via our filtering as per our AI policy (see TPFAT AI Policy)

User Profile and Device Management: Only school-provided email accounts will be used on Chromebooks; personal Gmail accounts will be blocked to prevent students from hiding online activity or bypassing school safety filters. Each student will be assigned a numbered Chromebook so teachers can monitor their work and online use.

This policy will be reviewed every year by the CEO who will consult senior leaders. At every review, the policy will be shared with the Board of Directors. The Online Safety Audit

(such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks children face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly. Schools will complete the Online Safety audit annually, and the effectiveness of filtering and monitoring provisions will also be reviewed at least annually to ensure they meet safeguarding needs, as required by Keeping children safe in education 2026.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

22. Links with other policies and Legislation

This online safety policy is linked to:

- Child Protection and Safeguarding Policy
- Positive Behaviour policy
- Anti-Bullying Policy
- Wellbeing Policies for staff and Pupils
- Digital Strategy Policy
- Data Protection Policy
- Complaints Policy
- Safe Handover/Children Walking Home Policy
- Staff Code of Conduct
- TPFAT ICT, Internet and Email Acceptable Use Policy
- TPFAT CCTV Policy
- TPFAT Freedom of Information Policy
- TPFAT Internet and Email Policy
- TPFAT Remote Learning Policy
- TPFAT Social Media Policy
- TPFAT Home School Partnership: Keeping Things Positive
- TPFAT Whistle-blowing Policy
- TPFAT Use of Artificial Intelligence Policy
- TPFAT Mobile Phone Policy
- Keeping Children Safe in Education 2026

Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers)

ACCEPTABLE USE OF THE ACADEMY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR CHILDREN AND PARENTS/CARERS

Name of pupil:

When I use the academy's IT systems (like computers) and get onto the internet in the academy I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use academy computers for school work only
- Be kind to others and not upset or be rude to them; the words I use/type will be kind, polite and sensible.
- Look after the academy's IT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given and I will try my hardest to remember my username and password
- Never give my personal information (my name, password, pictures, videos, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Check with my teacher before I print anything
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not look at or delete other people's files.
- I will not give my home address, phone number, send a photograph or video, or give any personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only previous met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I know that the academy may check my computer files and Google Classroom, and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet, parts of the Google Classroom.
- Save my work on the academy network and log off or shut down a computer when I have finished using it.

The use of mobile phones and smart devices in school:

- I know that I am not allowed to bring mobile phones or other smart devices, such as tablets and smart watches, into school.
- If I have a mobile phone for a medical reason, I will only use it for medical purposes.

I agree that the academy will monitor mobile phone use, the Google Classroom and the websites I visit and that there will be consequences in line with the Positive Behaviour Policy, if I don't follow the rules.

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE ACADEMY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR CHILDREN AND PARENTS/CARERS	
Parent/carer agreement: I agree that my child can use the academy's IT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for children using the academy's IT systems and internet, and will make sure my child understands these. I have read and understand the academy rules for Responsible Internet Use and give permission for my child to access the internet and the online learning platform, Google Classroom. I understand that the academy will take all reasonable precautions to ensure children cannot access inappropriate materials, while staff will employ appropriate teaching practice and teach online safety skills to children. I understand that my child's teacher will review these rules and ask each child in the class to sign a class agreement to adhere to them. I understand that the academy cannot be held responsible for the nature or content of materials accessed through the Internet. I will support the academy by promoting safe use of the Internet and digital technology at home and will inform the academy if I have any concerns over my child's online safety. I know that the academy has access to free online safety information for parents/carers and carers through National Online Safety and I can access this, and sign up using the following link. https://nationalonlinesafety.com/enrol/james-elliman-academy	
Signed (parent/carer:	**Date:**

Appendix 2: KS2 acceptable use agreement (children and parents/carers)

ACCEPTABLE USE OF THE ACADEMY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR CHILDREN AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the academy's IT systems (like computers) and get onto the internet in the academy I will:

- Always use the academy's IT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number, pictures or videos to anyone, or give any personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission. Without the permission of my teacher or parent/carer.
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Save my work on the network and always log off or shut down a computer when I've finished working on it
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will only email people I know, 'physical known people', not people I only know 'on line', or whom my teacher has approved.
- I will ask for permission before opening an email or an email attachment sent by someone I do not know.
- The messages I send will be kind, polite and sensible.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet, parts of the Google Classroom, or my email address.
- I will adhere to the academy's Digital Strategy User Agreement regarding the safe and responsible use of Chromebooks and all other digital devices and systems.

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the academy's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- I will not look at or delete other people's files.
- I will never arrange to meet someone I have only previous met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

If I bring a personal mobile phone or other personal electronic devices, such as tablets or smart watches, into the academy:

- I will not use it during lessons, break times and lunchtimes, clubs or other activities organised by the academy and I will hand it into the school office. I know it will be stored safely in the school office and I will collect it at the end of the day.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.
- If I have a mobile phone for a medical reason, I will only use it for medical purposes.
- **I agree that the academy will monitor mobile phone use, the Google Classroom and the websites I visit and that there will be consequences in line with the Positive Behaviour Policy, if I don't follow the rules.**

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE ACADEMY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR CHILDREN AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the academy's IT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for children using the academy's IT systems and internet, and for using personal electronic devices in the academy, and will make sure my child understands these. I have read and understand the academy rules for Responsible Internet Use and give permission for my child to access the internet and the online learning platform, Google Classroom. I understand that the academy will take all reasonable precautions to ensure children cannot access inappropriate materials, while staff will employ appropriate teaching practice and teach online safety skills to children. I understand that my child's teacher will review these rules and ask each child in the class to sign a class agreement to adhere to them. I understand that the academy cannot be held responsible for the nature or content of materials accessed through the Internet. I will support the academy by promoting safe use of the Internet and digital technology at home and will inform the academy if I have any concerns over my child's online safety. I know that the academy has access to free online safety information for parents/carers and carers through National Online Safety and I can access this, and sign up for free using the following link. https://nationalonlinesafety.com/enrol/james-elliman-academy	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, trainee teachers, Academy Council members, Board Directors, volunteers and visitors)

ACCEPTABLE USE OF THE ACADEMY'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, ACADEMY COUNCIL MEMBERS, BOARD DIRECTORS, VOLUNTEERS AND VISITORS	
Name of staff member/Academy council member/Board Director/volunteer/visitor:	
When using the academy's IT systems and accessing the internet in the academy, or outside the academy on a work device (if applicable), I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the academy's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network ● Share my password with others or log in to the academy's network using someone else's details ● Take photographs of children using personal devices. Any agreed photographs will be taken on school devices only and by an approved member of staff. ● Share confidential information about the academy, its children or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the academy **If I bring a personal mobile phone or other personal electronic devices, such as tablets or smart watches, into the academy:** ● I will not use it, for personal reasons, in the presence of children, during lessons, break times and lunchtimes, clubs or other activities organised by the academy. ● I will ask permission from the Principal if I need to access my phone or device, for personal reasons, during the school day and will use this away from children. ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating.	
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the academy's most recent online safety policy, Government/DfE Guidance and all other related policies. I wish to have an email account; be connected to the Intranet, Remote Access & the Internet; and be able to use the academy's IT resources and systems in accordance with the relevant policies. I will only use the academy's IT systems and access the internet in the academy, or outside the academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the academy will monitor the websites I visit and my use of the academy's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy. I will adhere strictly to the academy's specific guidance on the acceptable use of Generative Artificial Intelligence (AI) tools, as outlined in the Artificial Intelligence policy. I will let the designated safeguarding lead (DSL)/Deputy Designated Safeguarding Leads (DDSLs), IT Network Manager and the Online Safety Lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the academy's IT systems and internet responsibly, and ensure that children in my care do so too.	
Signed (staff member/Academy Council member/ Board Director/volunteer/visitor):	**Date:**

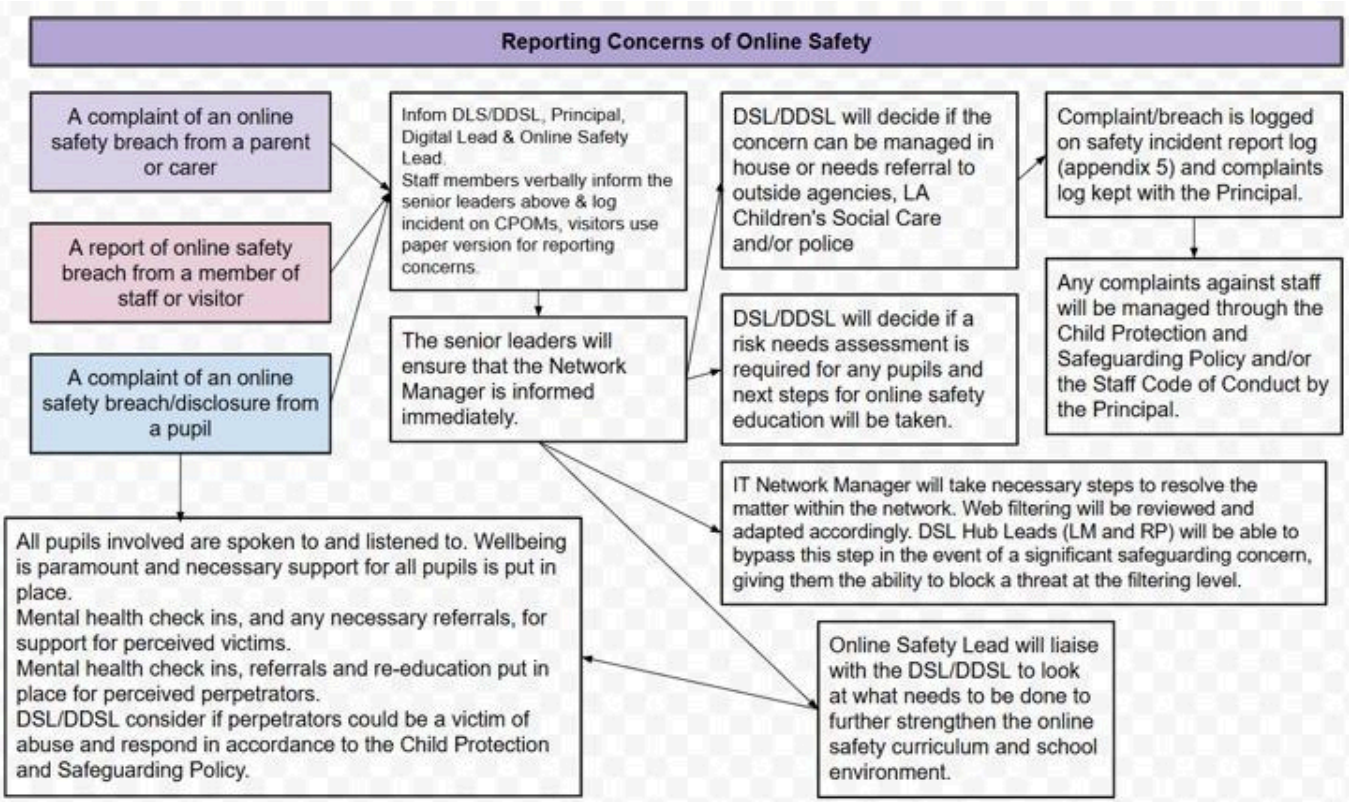
Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in the academy?	
Are you aware of the ways children can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, Academy Council members, Board Directors, volunteers and visitors?	
Are you familiar with the academy's acceptable use agreement for children and parents/carers?	
Do you regularly change your password for accessing the academy's IT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 6: Flowchart for reporting concerns around online safety


Reporting Concerns of Online Safety
A complaint of an online safety breach from a parent or carer
A report of online safety breach from a member of staff or visitor
A complaint of an online safety breach/disclosure from a pupil
Infom DLS/DDSL, Principal, Digital Lead & Online Safety Lead.
Staff members verbally inform the senior leaders above & log incident on CPOMs, visitors use paper version for reporting concerns.
The senior leaders will ensure that the Network Manager is informed immediately.
DSL/DDSL will decide if the concern can be managed in house or needs referral to outside agencies, LA Children's Social Care and/or police
DSL/DDSL will decide if a risk needs assessment is required for any pupils and next steps for online safety education will be taken.
Complaint/breach is logged on safety incident report log (appendix 5) and complaints log kept with the Principal.
Any complaints against staff will be managed through the Child Protection and Safeguarding Policy and/or the Staff Code of Conduct by the Principal.
IT Network Manager will take necessary steps to resolve the matter within the network. Web filtering will be reviewed and adapted accordingly. DSL Hub Leads (LM and RP) will be able to bypass this step in the event of a significant safeguarding concern, giving them the ability to block a threat at the filtering level.
All pupils involved are spoken to and listened to. Wellbeing is paramount and necessary support for all pupils is put in place.
Mental health check ins, and any necessary referrals, for support for perceived victims.
Mental health check ins, referrals and re-education put in place for perceived perpetrators.
DSL/DDSL consider if perpetrators could be a victim of abuse and respond in accordance to the Child Protection and Safeguarding Policy.
Online Safety Lead will liaise with the DSL/DDSL to look at what needs to be done to further strengthen the online safety curriculum and school environment.

Appendix 7: Staff handout of the Federations Approach to Filtering and Monitoring

Federation Approach to Web Filtering: Information Sheet

Web-filtering and Monitoring Arrangements at The Park Federation Academy Trust

Rationale

The Park Federation Academy Trust ensure that online safety is of the highest priority in order to keep children safe in an online world.

Our aim is to ensure all children:

- are safe when using technology in school through robust web filtering and monitoring systems that are regularly reviewed
- are aware of how to keep themselves safe when online outside of school
- can identify the online risks, including the risks of Generative AI
- know what to do and who to go to if they feel unsafe online

What are web-filtering and monitoring systems?

Web-filtering and monitoring systems provide a safe environment to learn and work by protecting pupils and staff from harmful and inappropriate content online. What's seen to be harmful will depend on each pupil.

What's my role?

All staff need to:

- Follow policies and procedures as outlined in the Child Protection and Safeguarding Policy, the Online Safety Policy, and any other school policies that relate to online behaviours and safety
- Report any problems to the Principal, DSL/DDSL, Digital Lead and Online Safety Lead
- Monitor what's happening on screens, both physically and through the use of Senso

Who's responsible for our system and procedures?

- The DSL/DDSL takes lead responsibility for filtering and monitoring reports and any safeguarding concerns that appear
- The Senior leadership team makes sure staff understand their roles, reviews the effectiveness of our systems and oversees reports
- IT service provider, LGfL Webscreen, has technical responsibility for maintaining and managing our system
- In addition to LGfL Webscreen, we also use **YouTube Strict, Google Safe Search and Senso** to ensure staff are alert to potential safeguarding concerns and harmful content.
- Chrome Books also have whole class monitoring mode so that class teachers can see what pupils are accessing during lessons.

What to do if you feel filtering systems have been breached

If a member of staff becomes aware of a breach they MUST report it to the following members of school staff immediately:

- **Principal**
- **DSL/DDSL**
- **Online Safety Lead**
- **Digital Lead**
    - **These senior leaders will them alert the Network Manager**

Network Manger will take necessary steps to resolve the matter within the network.

- DSL Hub Leads (LM and RP) will be able to bypass this step in the event of a significant safeguarding concern, giving them the ability to block a threat at the filtering level.
- The device will be removed from use whilst the concern is being investigated.
- Access to the internet may be restricted during the investigation.
- Nominated school staff will support children/staff members impacted by this by providing online safety education and pastoral support.
- Parents will be informed and the incident logged on CPOMs if appropriate
- Children will be praised for reporting concerns.
- The schools DSL will follow the Child Protection and Safeguarding Policy and the Online Safety Policy.

What do we mean by a breach?

- A breach may be inappropriate material that has been seen, or reported to have been seen, on any school device. This could be by staff or children. This could be deliberate or accidental.
- A breach could be a child being seen, or reported to have been seen, searching for or viewing inappropriate material on a school device.
- The Network Manager will take appropriate steps to ensure that the web filtering systems are working appropriately.
- The Network Manager will review categories that are blocked and not blocked to ensure that web filtering is working appropriately.
- The Network Manager will inform appropriate staff when the concern has been addressed, including the CEO.
- Internet and device usage will resume once the matter has been resolved and/or the web filtering system is deemed safe for use.

How is information on web-filtering and monitoring communicated between the school and the Network Manager

Each term, there is a federation web-filtering and monitoring meeting between the the CEO -, Helen Abell, DSL Hub Lead for Slough - Rebecca Pinkney, DSL Hub Leads for Hillingdon - Lorna Mitchell, Safeguarding Representative for the Board - Ranisha Dhamu, Federation Digital Lead - Carolyn Hillarious and the Federation Network Manager – Chris Newton. During these meetings the following is discussed and reviewed:

- A review of the categories available to staff and pupils and what is blocked and not blocked - the team will decide if any changes need to be made.
- A decision on whether any schools have felt there has been any over blocking in their academies.
- A summary from the Network Manager on any breaches reported at any

school, cyber attacks or any filtering and monitoring problems or developments have arisen.

- As a team any patterns and trends will be discussed
- Hub DSLs then disseminate this information to their DSLs and Principals.

Where should I go if I need to remind myself of this information?

You can find these details in the appendices of our Child Protection and Safeguarding Policy and our Online Safety Policy on our website.

Information for schools can also be found here - Meeting the standard