PACE Academy Trust

CVPS

PACE Academy Trust

Online Safety (inc Social Media) Policy

Chipstead Valley Primary School

UN Convention on the Rights of the Child

Article 17 – Children have the right to collect information from the media They should also be protected from information that could harm them.
Article 19 – Children have the right to be protected from being hurt or badly treated.

Document Control Table

Document Title	Online Safety (inc Social Media) Policy (PACE Schools)
Author	Trust Designated Safeguarding Leads
Version number:	3
Date approved:	24th September 2025
Approved by:	PACE Strategic Board

Document History:

Version	Date	Author	Note of revisions
1		DSL	
2	Summer 025	DSLs/ZH	Updated to reflect KCSiE 2024
3	Autumn 2025	ZH	Updated to reflect KCSiE 2025

Contents

Contents 2

Process for monitoring the impact of the Online Safety Policy 3

Key Contacts 4

Introduction 5

Local Concerns 5

Introduction and Aims 6

Scope 7

Roles and responsibilities 7

- Headteacher and other Executive Leaders 7
- Designated Safeguarding Lead / Online Safety Lead 8
- Governors 9
- All Staff 9
- Pupils 10
- Parents/Carers 11

Network Manager –OpenAir 11
Data Protection Officer (DPO) - OpenAir 12
Volunteers, Visitors and Contractors 12
External Groups including those hiring the premises and PTAs. 12
Online Safety and the Curriculum 12
Handling Online-Safety Concerns and Incidents 13
Nudes – sharing nudes and semi-nudes 14
Bullying 15
Child-on-child Sexual violence and sexual harassment 15
Upskirting 15
Extremism 15
Electronic communication - Email 16
Use of generative Artificial Intelligence (AI) 16
Cloud Platforms 16
Digital Images and Video 17
Social Media 18
Social Media Incidents 19
Device Usage 19
Use of School Devices 20
Searching and Confiscation 21
CCTV 21
Data Protection and Cyber Security 21
Filtering and Monitoring 22
Filtering 22
Monitoring 22
Misuse of Technology 23

Process for monitoring the impact of the Online Safety Policy

This policy document is subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Acceptable Use Policies are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

The school will monitor the impact of the policy using:

- *logs of reported incidents*

- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

Key Contacts

	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Louise Bacon Kate Duncan
	Online-safety lead (if different)	N/A
	Deputy Designated Safeguarding Leads (DSL) team	Rebecca Herrera
	Online-safety / safeguarding link governor	Shelly Rowe
	Link governor for web filtering if different from above	N/A
	Curriculum leads with relevance to online safeguarding and their role e.g. PSHE/RSHE/RSE/Computing leads	Tom McMurray (Computing lead) Wellbeing curriculum lead (TBC Spring 1)
	Network manager / other technical support	OpenAir Systems
	Date this policy was reviewed and by whom	Spring 2025 PACE DSL team/ZH
	Date of next review and by whom	Summer 2026 - DSLs

Introduction

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach, and collaboration between key school leads. This Online Safety Policy outlines the commitment of PACE Academy Trust to safeguard members of our school community online in accordance with statutory guidance, best practice, and the Online Safety Act.

This policy is written in line with Keeping Children Safe in Education and other relevant statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and sits alongside other policies including:

- Safeguarding and Child Protection
- Behaviour
- Anti-Bullying and Anti-Discrimination

Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Local Concerns

Use of WhatsApp and Social Media Platforms for Inappropriate Communication: Risks of misuse by parents and children for sharing harmful, inappropriate, or abusive messages.

Online Grooming and Sexual/Criminal Exploitation: Risks of children being contacted by adults or peers with harmful intent via online platforms.

Cyberbullying and Peer-on-Peer Abuse: Bullying that moves from the classroom to online spaces, including group chats and social media.

Exposure to Harmful Content: Inappropriate material such as violence, pornography, or extremist content.

Sexting and Image Sharing: Concerns about children being pressured to share indecent images.

Radicalisation and Extremism: Online platforms being used to influence or radicalise young people.

Privacy and Data Protection: Risks around oversharing personal information online.

Mental Health Impacts: Links between excessive screen time, social media pressure, and anxiety or depression.

Introduction and Aims

PACE Academy Trust is committed to safeguarding children from potentially harmful and inappropriate online material. Our policy aims to ensure our stakeholders have an awareness of the breadth of issues classified within online safety. These are considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

contact: being subjected to harmful online interaction with other users; for example: child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This policy aims to promote a whole Trust approach to online safety by:

- Setting out expectations for all PACE community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Facilitating the safe, responsible, respectful, and positive use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform and that the same standards of behaviour apply online and offline.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.

- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.

Scope

This policy applies to all members of the PACE Academy Trust community (including teaching, supply and support staff, governors, directors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

PACE Academy Trust and its respective schools form a community, and all members have a duty to behave respectfully online and offline; to use technology for teaching and learning and to prepare for life after school; and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of the school.

Headteacher and other Executive Leaders

- Foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding.
- Oversee/work with colleagues to complete the GOV.UK self-assessment document: Plan technology for your school - GOV.UK and create a plan to address any recommendations that work towards meeting the digital and technology standards Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK
- Carrying out an annual review of their approach to online safety (a free online safety self-review tool for schools can be found via the 360 safe website or LGfL online safety audit)
- Ensure that policies and procedures are followed by all staff.
- Ensure all staff, parents, volunteers, and children are made aware of/sign the school's acceptable use policy (AUP) on an annual basis.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Take overall responsibility for data management and information security ensuring the school/trust provision follows best practice in information handling.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors and directors undergo safeguarding and child protection training and updates (including online safety) and that governors and directors are regularly updated on the nature and effectiveness of the school/trust's arrangements.
- Ensure the school/trust implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Ensure the trust's approach to filtering and monitoring is maintained — in particular, understand what is blocked or allowed for whom, when, and how.

- Monitor FortiGuard reports, raising any queries or concerns with the trust's Strategic Lead for Safeguarding/OpenAir.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.

Designated Safeguarding Lead / Online Safety Lead

- The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] and understanding the filtering and monitoring systems and processes in place and ensure an effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring and work with the headteacher and OpenAir to carry out reviews and checks on filtering and monitoring.
- Ensure the school complies with the trust's YouTube mode and preferred search engine/s etc.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit.
- Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and receive regular updates about online safety issues and legislation, being aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and do not dismiss it as banter (including bullying)
- Promote an awareness of and commitment to online safety throughout the school community.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated. This must include:
    - filtering and monitoring and help them to understand their roles.
    - all staff must read KCSIE Part 1 and all those working with children Annex B
    - cascade knowledge of risks and opportunities throughout the organisation

Governors

- Approve this policy and subsequently review its effectiveness.
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL to lead responsibility for safeguarding and child protection (including online safety)
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school.
- Ensure that all staff undergo safeguarding and child protection training (including online safety)
- Ensure appropriate filters and appropriate monitoring systems are in place, reviewing these at least annually
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Sign and follow the acceptable use policy (AUP) and code of conduct for governors.
- Ensure the school has completed the GOV.UK self-assessment document: Plan technology for your school - GOV.UK and has a plan to address any recommendations that work towards meeting the digital and technology standards Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK

All Staff

- Understand that online safety is a core part of safeguarding; it is part of everyone's responsibility– never that someone else will address it.
- Read and follow this policy in conjunction with the school's main safeguarding policy, Part 1, and Annex B of Keeping Children Safe in Education
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign and follow the staff acceptable use policy (AUP) and code of conduct.
- Notify the DSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon.

- Identify opportunities to integrate online safety through all school activities as part of a whole school approach in line with the RSHE curriculum.
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites.
- When supporting pupils remotely, be mindful of additional safeguarding considerations especially when using live-streaming or videoconferencing.
- Carefully supervise and guide pupils in activities involving online technology, helping them develop search skills, critical thinking, and understanding of copyright, plagiarism, and GDPR
- Monitor the use of digital devices such as mobile phones and cameras during school activities, ensuring compliance with school policies.
- In pre-planned lessons using the internet, guide students to appropriate websites and have processes in place to manage unsuitable content that may appear in searches.
- Always be aware of security best-practice, including password hygiene and phishing strategies.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to online bullying and sexual harassment and discrimination.
- Ensure all digital communication with learners and parents/carers is professional and conducted only through official school channels.
- Model safe, responsible, and professional behaviours in your own use of technology, including outside of school and on social media, upholding both the school's and your own professional reputation.

Pupils

- Read, understand, sign, and adhere to the pupil acceptable use policy.
- Treat home learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- Never engage in any private communication with school staff or tutors
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor and know how to do so.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/Carers

- Read, sign, and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers
- Support the school in reinforcing the online safety messages provided to learners in school.
- Support the school in the safe and responsible use of their children's personal devices -- through applying appropriate filters, monitoring and parental controls and ensuring age-appropriate apps and games.
- Support the school by not sending in personal devices for use in school.

Network Manager –OpenAir

It is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology and to support them to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.
- Work closely with the DSL and Online Safety Lead and DPO to ensure that the school's systems, networks, and devices reflect current policies and meet the required online safety standards.
- Support PACE schools in the completion of the GOV.UK self-assessment document: Plan technology for your school - GOV.UK and the creation of a plan to address any recommendations that work towards meeting the digital and technology standards Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Manage the school's systems, networks, and devices, applying strict password policies, protections, encryption, and backups for data.
- Ensure clear and managed control of user access to networks and devices, following the school's access policies.
- Monitor the use of school technology ensuring that any misuse or attempted misuse is identified and reported according to school policy.

- Report any online safety-related issues that come to their attention, in line with school procedures, to the relevant person.
- Monitor and update technical security and online safety systems regularly, ensuring ongoing compliance with school policies and safeguarding requirements.
- Work with the Data Protection Officer (DPO) to ensure that all data is handled securely, and all policies comply with data protection regulations.
- Work with the Headteacher to ensure the school website meets statutory DfE requirement.

Data Protection Officer (DPO) - OpenAir

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents such as 'Keeping Children Safe in Education' and Data protection in Schools 2023 to not prevent, or limit, the sharing of information for the purposes of keeping children safe.
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate.
- Provide data protection expertise and training.

Volunteers, Visitors and Contractors

- Read, understand, sign, and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Model safe, responsible, respectful, and positive behaviours in their own use of technology, including on social media.
- Maintain an awareness of current online safety issues and guidance.
- Support the school in promoting online safety and data protection.

External Groups including those hiring the premises and PTAs.

- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Support the school in promoting online safety and data protection.

Online Safety and the Curriculum

At PACE Academy Trust we recognise that online safety and broader digital resilience must thread throughout the curriculum. Despite the associated risks, we recognise the opportunities and benefits of

children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes.

Wellbeing and Computing Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme taught through the computing curriculum, PSHE and RSE schemes of work, assemblies, other pastoral programmes, and relevant national initiatives such as Safer Internet Day. Teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives. The online safety programme will cover:

- consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in generative artificial intelligence, financial extortion and sharing intimate pictures online.
- being taught about positive, healthy, and respectful online relationships and what these looks like, the effects of their online actions on others and knowing how to recognise and

The following subjects have the clearest online safety links:

- Relationships education, relationships, and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation, and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort led by the DSL.

Handling Online-Safety Concerns and Incidents

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

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies

- Prevent Risk Assessment
- Data Protection Policy, agreements, and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside and outside school and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on Every (PACE health and safety portal). This includes any concerns raised by the filtering and monitoring systems.

Any concern/allegation about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

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

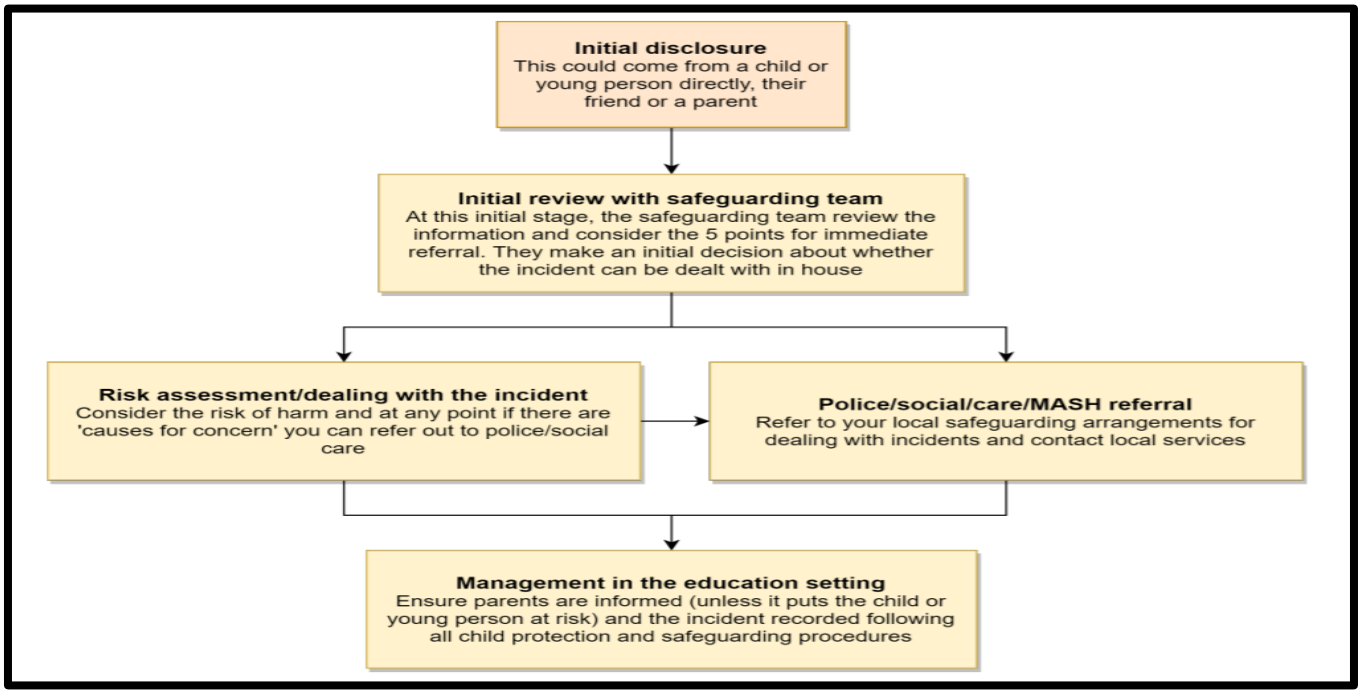
Nudes – sharing nudes and semi-nudes

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings and the one page overview of how to respond to an incident.

Staff other than the DSL must not attempt to view, share, or delete the image or ask anyone else to do so, but to go straight to the DSL.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area.

The school DSL will use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.



Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the PACE Anti-Bullying Policy should be followed. This includes issues arising from banter. It is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline element.

Child-on-child Sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL immediately. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here.' Schools must take all forms of sexual violence and harassment seriously, recognising how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Upskirting

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment As with other forms of child-on-child abuse pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages, or individuals, give them a voice or opportunity to visit the school; nor browse, download, or send material that is considered offensive or

of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Electronic communication - Email

Email is the official electronic communication channel between parents and the school, and between staff and pupils. Our Management Information System is used to send texts and email communication from the school to parents but not to receive them.

Staff at this school use the Microsoft 365 system, Egress and Arbor for all school emails. Email systems used by staff are fully auditable and trackable. This is for the mutual protection and privacy of all staff, pupils, and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, Tapestry and Microsoft Teams are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions).
- Email sent by staff may only be sent using the systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, this should be password protected or sent securely using USO-FX or Egress systems.
    - Internally, staff should use the school network (Microsoft 365) including when working from home to share information.
- Appropriate behaviour is always expected. The system must never be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read, and the same rules of appropriate behaviour always apply.

Use of generative Artificial Intelligence (AI)

At PACE we acknowledge that generative AI platforms (e.g. ChatGPT, Canva, Co-Pilot etc) are becoming widespread. We are aware of and follow the DfE's guidance on this, along with our own guidance on the use of AI. In particular:

- We will talk about the use of these tools with pupils, staff, and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI to plagiarise is prohibited.

Cloud Platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

The following principles apply:

- Training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used by students or staff to store pupil work.

Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name. Photo file names/tags do not include full names to avoid accidentally sharing them.

At PACE Academy Trust, no member of staff will ever use their personal phone to capture photos or videos of pupils except in the rarest of circumstances. These circumstances must always be agreed with the DSL/DPO and Headteacher, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually and at each public performance about the importance of not sharing without permission, due to reasons of child protection and data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated and are advised to be incredibly careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of

the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social Media

PACE Academy Trust works on the principle that if we do not manage our social media reputation, someone else will. Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online. We manage and monitor our social media footprint carefully to know what is being said about the trust and school and to respond to criticism and praise in a fair, responsible manner.

Social media is a fact of modern life, and as a school, we accept that many parents, staff, and pupils will use it. However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages, or groups.

If parents have a concern about the school, we urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils, and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of thirteen, but the school regularly deals with issues arising on social media with pupils who are 11yrs or younger. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. This include online games such as RoBlox, which also has a social media element to it and is popular amongst primary aged children.

However, the school must strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation, or abuse. Children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). The following resources are shared with parents annually: Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Class WhatsApp groups and other WhatsApp groups maintained by parents, members of a parent/teacher association, or similar, must adhere to the remits of this policy.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers, and contractors or otherwise communicate via social media.

Pupils should not 'follow' staff, governor, volunteer, or contractor public accounts (e.g. following a staff member with a public Instagram account). In the reverse situation, staff must not follow any student accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school, or its stakeholders, on social media and be careful that their personal opinions might not be attributed to the school, trust, or local authority, and could bring the school into disrepute.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Social Media Incidents

Breaches will be dealt with in line with the school safeguarding procedures and behaviour policy (for pupils) or code of conduct (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Device Usage

Pupils are allowed to bring mobile devices in for emergency use only. Any attempt to use a mobile device in lessons without permission or to take illicit photographs or videos will lead to the withdrawal of the mobile device and consequences in line with the school's behaviour policy. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

Pupils are not allowed to wear 'wearable technology' such as smart watches as these have camera and recording facilities.

Where **home devices are** issued to some students, these are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked.

All staff who work directly with children should leave their mobile phones on silent and only use them during school hours in private staff areas. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

For school trips/events away from school, teachers may be issued a school duty phone, and this number is used for any authorised or emergency communications with parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Volunteers, visitors, contractors, governors should leave their phones in their pockets/bags and set to silent mode. Under no circumstances should they be used in the presence of children or to take photographs or videos without explicit permission from the headteacher (and this should be done in the presence of a member staff). Volunteers, visitors contractors and governors can access the guest wireless network but must have no access to networked files/drives, subject to the acceptable use policy.
All internet traffic is monitored.

Parents are asked to leave their phones in their pockets and on silent mode when they are on site or attending a school trip. Parents who assist with school trips /events should limit their phone usage to essential communication only. Parents must ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. Parents have no access to the school network or wireless internet on personal devices.

Use of School Devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct. Wi-Fi is accessible for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning as well as appropriate personal use. All and any usage of devices and/or systems and platforms may be tracked.

Searching and Confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', Executive leaders and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example because of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence, or bullying.

CCTV

Chipstead Valley Primary School currently operates 12 CCTV cameras around the external site. These cameras are in place to support safeguarding and ensure the safety of pupils, staff and the premises. Gates and doors are monitored to record who enters and exits the building at any given time.

All footage is securely stored for 30 days before being automatically deleted. Access to recorded footage is restricted to a small number of authorised staff and is only viewed when necessary.

To maintain transparency, we display clear signage on windows and doors to inform everyone that CCTV is in operation

Data Protection and Cyber Security

All pupils, staff, governors, volunteers, contractors, and parents are bound by the school's data protection and cyber security policies.

The executive leaders across PACE, data protection office and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first, and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should always treated with the strictest confidentiality and only shared via approved channels to colleagues or agencies with appropriate permissions.

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times) or live supervision by staff on a console with device management software
2. Internet and web access: network monitoring using log files of internet traffic and web access.
3. Active/proactive technology monitoring services

At PACE, we combine all three aspects of monitoring.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the headteacher and OpenAir. A Data Protection Impact Assessment must be completed for all new platforms or apps that store school/child data.

Filtering and Monitoring

The DSL has lead responsibility for filtering and monitoring and works closely with senior leaders, governors and the IT Service Provider to agree the school filtering and monitoring provision and regularly review and update it in response to changes in technology and patterns of online safety incidents/behaviours. The IT service provider will have the technical responsibility.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking.

Across PACE, we utilise the FortiGate Firewall with FortiGuard in conjunction with the LGfL filtering service to provide robust filtering and monitoring of the school's IT infrastructure. This system is designed to ensure a secure online environment by blocking unauthorised and harmful content while generating alerts for any potential breaches or inappropriate activity. Together, these tools help maintain compliance with online safety policies, ensuring the protection of both students and staff.

Filtering

- the school manages access to content across its systems for all users and on all devices that use the school's internet provision. This includes any personal device that is connected to the school's Wi-Fi system. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school has monitoring systems in place to protect the school, systems, and users:

- The school monitors all network use across all its devices and services.

- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead and Headteacher to breaches of the filtering policy, which are then acted upon.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead.
- all users are aware that the network (and devices) are monitored. This includes persona devices that connect to the school's Wi-Fi system.
- There are effective protocols in place to report abuse/misuse.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

Misuse of Technology

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Code of Conduct and Acceptable Use Policies as well as in this document.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.