Pilgrims School

Online-Safety Policy

October 2022

Next review date: October 2023

Table of Contents

School Name and contact details	Pilgrims Pre-Preparatory School Brickhill Drive Bedford MK40 3SJ Tel: 01234 369555
Designated Safeguarding Lead /Online-Safety Lead and contact details	Mrs Tracey Marquand t.marquand@pilgrims-school.org.uk
Deputy Designated Safeguarding Leads and contact details	Mrs Zoe Miles z.miles@pilgrims-school.org.uk Miss Justyna Kuzio j.kuzio@pilgrims-school.org.uk
Chair of Governors	Mrs Sarah Wheeler s.wheeler@pilgrims-school.org.uk
Designated Governor for Safeguarding and contact details	Reverend Lucy Davis lucy.davis@pilgrims-school.org.uk
Chief Executive of the Harpur Trust	David Steadman – Tel Harpur Trust Office : 01234 369500
Designated Lead for Pastoral and SEND	Mrs Jacqueline Morales j.morales@pilgrims-school.org.uk
PSHCEE Lead	Mr Graham Orr g.orr@pilgrims-school.org.uk
Marketing Co-ordinator	Karen Sinclair k.sinclair@pilgrims-school.org.uk
Reviewed annually, date last reviewed	New policy
Signed by Chair of Governors	

Please note: 'School' refers to Early Years Foundation Stage (Little Pilgrims, Kindergarten and Pre School) and Pilgrims Main School.

1. Introduction and Ethos

We believe that:

- children should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children safe online, whether or not they are using our school network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, their parents, carers and other agencies is essential in promoting children's welfare and in helping them to be responsible in their approach to online safety

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing subjects including PSHCEE and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

What are the main online safety risks today?
Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022):

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; 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: 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, and
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel children or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

These areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between them. KCSIE 2022 highlights additional risks e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their

families, including sexual and criminal exploitation, serious youth violence, upskirting and sticky design.

Remote learning increases the risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that pupils may miss opportunities to disclose such abuse during periods of absence from school.

2. Aims

This policy aims to:

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

Scope

This policy applies to all members of our school community (including teaching and support staff, supply teachers, governors, volunteers, contractors, 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.

3. Roles and responsibilities

This school is 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. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher - Mrs Jo Webster

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.

- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below, including working with technical colleagues to complete an online safety audit in line with KCSIE, are being followed and fully supported.
- Support safeguarding leads, technical and other staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Ensure the school's data management and information security practices are in line with the Harpur Trust's Data Protection Policy; work with the Trust's Data Protection Office (DPO), the DSL and governors to ensure implementation of a GDPR-compliant framework for storing data in accordance with the Harpur Trust's Data Protection Policy.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how.
- Ensure all staff undergo safeguarding training (including online safety) at induction with regular updates.
- Ensure all governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- 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 the needs of pupils, including risk of children being radicalised.
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Lead – Mrs Tracey Marquand

Key responsibilities:

- Take lead responsibility for safeguarding and child protection [including online safety]. This lead responsibility should not be delegated.
- Ensure an effective whole school approach to online safety.
- Ensure all staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
- Liaise with the Headteacher and Chair of Governors to ensure that all governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).

- Liaise with staff (especially pastoral support staff, the school nurse, IT Technicians, and the SENCO, on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work with the headteacher, Harpur Trust's DPO and governors to ensure implementation of a GDPR-compliant framework for storing data, in accordance with the Harpur Trust's Data Protection Policy.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends and the latest trends in online safeguarding and undertake Prevent awareness training.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor to discuss current issues (anonymised), review incident logs and, along with the IT Technicians review filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware. Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE "be careful that 'over blocking' does not lead to unreasonable restrictions".
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex B
  - cascade knowledge of risks and opportunities throughout the organisation
- Pay particular attention to online tutors hired by parents, share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles.

Governing Body, led by Online Safety / Safeguarding Link Governor – Reverend Lucy Davis

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2022)

- 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.
- Ask about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards.
- "Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection

(including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- 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.
- Work with the Harpur Trust's DPO, DSL and headteacher to ensure implementation of a GDPR-compliant framework for storing data, in accordance with the Harpur Trust's Data Protection Policy.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and that training is regularly updated.
- Ensure appropriate filters and appropriate monitoring systems are in place.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

All staff

Key responsibilities:

- Recognise that RSHE is statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this subject.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL) is.
- Read Part 1of Keeping Children Safe in Education and school leaders and staff that work directly with children should also read Annex B.
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- 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 (find out what appropriate filtering and monitoring systems are in place).
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using.
- Encourage KS1 pupils to follow their acceptable use policy at home as well as at school.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know.

- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Subject leaders to look for opportunities to embed online safety elements.

PSHCEE Lead – Mr Graham Orr

Key responsibilities:

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

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCEE / 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. 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 to 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. This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCEE.
- Note that an RSHE policy should now be included 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.
- Keep teaching staff, including the computing subject lead up to date with any updates or changes to the curriculum in accordance with the national curriculum.

Computing Lead – Mr David Carr

Key responsibilities:

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

- Work closely with the PSHCEE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/OSL and all other staff to ensure an 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.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.

Network Manager/technician – IT Department at Bedford School

Key responsibilities:

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

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.

- Support the DSL and SLT to carry out an annual online safety audit as recommended in KCSIE. Including a review of technology, filtering and monitoring systems, protections for pupils in the home and remote learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- Report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Monitor the use of school technology, and that any misuse/attempted misuse is identified and reported in line with school policy.

Data Protection Officer (DPO) – Finance Director at Harpur Trust

Key responsibilities:

- Ensure that Harpur Trust's Data Protection Policy reflects the relationship between data protection and safeguarding.
- Ensure the Harpur Trust's Record and Retention Policy reflect the requirements to retain safeguarding records in accordance with KCSIE.
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing.
- With the DSL and IT department, ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors

Key responsibilities:

- 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.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Pupils in KS1 to read, understand, sign and adhere to the pupil acceptable use policy and review this regularly and at a minimum annually.

- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings 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.
- 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.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media.
- 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

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the KS1 pupil AUP and encourage their children to follow it when they enter Year 1.
- 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.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns.
- Support their child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure their child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure their child knows tutors should not arrange new sessions directly with them or attempt to communicate privately.

External groups including Pilgrims Parents' Association

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- 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.

4. Handling online-safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHCEE). General concerns must be handled in the same

way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

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

- Safeguarding Children Policy
- Anti-Bullying Policy
- Behaviour Assertive Discipline Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment

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 online safety lead / designated safeguarding lead by logging a concern through the Wellbeing Module on iSAMS.

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 (Mrs Sarah Wheeler). Staff may also use the NSPCC Whistleblowing Helpline. In all cases, the Local Authority Designated Officer (LADO) and the Chief Executive of the Harpur Trust should be notified.

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

Sharing nudes and semi-nudes

In the latest guidance for schools (UKCIS, 2020) this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. And must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

It is usually someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. 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 following our school safeguarding procedures. Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal.

If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to) report this to the DSL and seek support. The school DSL will in turn 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.

At initial review the DSL should consider the following 5 points for immediate referral:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

Upskirting
All staff are aware of the criminal act of 'upskirting' defined by the Criminal Prosecution Service as a colloquial term referring to the action of placing equipment such as a camera or mobile phone beneath a person's clothing to take a voyeuristic photograph without their permission. It is not only confined to victims wearing skirts or dresses and equally applies when men or women are wearing kilts, cassocks, shorts or trousers. It is often performed in crowded public places, for example on public transport or at music festivals, which can make it difficult to notice offenders.

Bullying
Online bullying, including incidents that take place outside school or from home, should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Sexual violence and harassment
Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

5. Education and curriculum

PSHCEE and Computing are the subjects that have the clearest online safety links however we recognise that online safety and broader digital resilience must be thread throughout the curriculum. As stated in the role descriptors above, it is the role of all staff to identify opportunities to facilitate this. We are also working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). Annual reviews of curriculum plans / schemes of work are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including remote teaching), supporting them with search skills, critical

thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

6. Online learning

Staff engaging with pupils and /or parents online have a responsibility to model safe practice at all times. It is the responsibility of the staff member to act as moderator. Staff will adhere to the Code of Conduct and this Online-Safety policy.

Susan Quince (Deputy Headteacher) is responsible for co-ordinating the whole school online learning approach with support from Jo Webster (Headteacher), Tracey Marquand (Designated Safeguarding Lead), David Carr (IT Teacher) and expert guidance from The IT Department at Bedford School. They have risk assessed and reviewed potential safeguarding issues created by teaching online.

We have a whole school approach to online teaching and one-to-one tuition online is not permitted unless it has been authorized by the headteacher and agreed in advance with parents. The following ways of communicating with children and supplying online learning are utilized:

- Purple Mash – lesson plans and pre-recorded videos are available for parents and children. All children from Reception upwards have their own Purple Mash login account.
- Pilgrims closed Facebook Page which is monitored closely be Karen Sinclair.
- Use of Microsoft Teams for teaching. Only Pilgrims Teachers can contact the children as Teams is a closed ecosystem requiring Pilgrims Accounts. This service enables teachers to disable microphones and video cameras if needed however there is a level of parental responsibility involved to ensure that their child is using the service responsibly.
- The Team meetings will be recorded and held within the team meeting for 21 days. They will automatically delete after this period of time.
- If the videos need to be kept for any reason e.g. a safeguarding concern, they will be downloaded and then uploaded into Stream.
- All members of a meeting can watch the recording after it has finished for 21 days. If for any reason, for example safeguarding, access to the video needs to be restricted staff would need to download the video and delete it from the Teams meeting.
- Children also have access to pre-recorded videos on Stream through embedded URL links which are accessed on their daily timetables in Purple Mash.
- Staff must use their school email address when communicating with parents.
- If staff need to contact a parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and if there is no alternative always use 'caller withheld' to ensure the parent is not able to identify the staff member's personal contact details.

Training on the systems identified above is provided to staff. The IT Department at Bedford School in liaison with David Carr provide the technical knowledge to maintain safe IT arrangements. Teams / Stream and Purple Mash are closed ecosystems, so we control access and content. The Harpur Trust have risk assessed the use of live learning using webcams. Internet usage and filtering at home is the responsibility of the parent and we advise parents to check their security provisions at home.

School Safeguarding Procedures during online teaching
During any online teaching our usual Safeguarding guidelines continue to apply however we recognise that communicating online may allow us a view into a young person's world that we would not have seen at school. This may generate some safeguarding concerns for that child.

Whilst working remotely and communicating online with children and parents we will continue to follow our regular safeguarding processes.

Additional considerations for online tuition:

- Avoid one to one online tuition to help safeguard children and staff.
- Staff must wear suitable clothing, as should anyone else in the household who may inadvertently walk past the online session.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background. Backgrounds if possible, should be blurred.
- The live class should be recorded by the member of staff initiating the session and stored on Streams, so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Resources and videos must be age appropriate. Staff must check the suitability of any online source that they recommend.
- If a member of staff is unable to run a live session, due to ill health for example, they must advise their line manager. Alternative cover for the session will then be provided by either Jo Webster, Susan Quince or Kim Goodwin.

7. Misuse of school technology (devices, systems, networks or platforms)

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 Acceptable Use Policy as well as in this document.

- School laptops are Trust/School property, they are for staff use only, and every care should be taken to ensure they are not lost, stolen or damaged.
- Staff may use their own equipment when working remotely however the user is responsible for ensuring security of equipment on their Network / Internet connection.
- Staff must work from a secured space at home as opposed to using any kind of public WiFi network. Any work-based systems or databases should be accessed directly via the work portal only, to ensure that the relevant protection is in force and to prevent any security breaches.
- Staff should use only trusted sources for any information and be particularly cautious of junk mail and phishing attempts. If staff have any questions, or notice something suspicious on their computer or work phone they must immediately contact IT.

GDPR

It is important to keep all business information confidential whilst working at home in the same way as it is within the workplace. This includes ensuring other household members do not have access to any confidential information, ensuring that relevant passwords are used and screens are locked if staff are not at their computer. The Data Protection Policy and Information Security Policy will still apply, and staff are advised to read these policies prior to working from home.

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

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

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.

8. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Karen Sinclair the school's marketing co-ordinator. The site is hosted by Unity Limited and managed by Prominent PR under the supervision of the school's marketing co-ordinator:

The DfE has determined information which must be available on a school website. When placing information on the website the following must be considered:

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches.
- Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

9. Social media

Our school works on the principle that if we don't manage our social media reputation, someone else will. Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school. Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. Our marketing co-ordinator is responsible for managing our closed Facebook account and Prominent PR manage our public Twitter/Facebook/Instagram accounts and check our Wikipedia and Google reviews.

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies for all members of the school community, 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 (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

Staff social media presence
Staff including volunteers must not publish anything which could identify pupils, parents or guardians on any personal social media account, personal webpage or similar platform. This includes photos, videos, or other materials such as pupil work.

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 or trust, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 333 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the staff Code of Conduct.

Parents' social media presence
If parents have a concern about the school, we would 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). We will respond to general enquiries about the school via social media but email is the official electronic communication channel between parents and the school.
We would also remind parents that we encourage children 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).

Children's social media presence
Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school does deal with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils 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 who to talk to if they are worried about anything they see. However, 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 children in our school are below the age restriction for using a social media account. 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 are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* 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 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.

10. Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the Trust's Data Protection Policy.

Rigorous controls on the school network, firewalls and filtering all support data protection.

The headteacher/principal, data protection officer 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 be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

11. Appropriate filtering and monitoring

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."

At this school, the internet connection is provided by a Tier 1 UK provider over a diverse route from 2 independent infrastructure partners. This means we have a dedicated, redundant, and secure, school safe connection that is protected with industry leading firewalls and multiple layers of security, including a content filtering system from a best of breed provider, which is made specifically to protect children in schools.

12. Electronic communications

- Staff at this school use the Microsoft Office 365 and /or iSAMS for all school communications.
- Pupils in Year 2 use Purple Mash to email during specific ICT lessons but it is turned off by default. They have a Microsoft Office 365 account, but this is only used to invite them to

online Teams meetings when accessing home learning. These accounts cannot be used to email external accounts.

Office 365 and iSAMS are fully auditable, trackable, and managed by Bedford School on behalf of the school. Purple Mash is also fully auditable, trackable, and managed by Pilgrims School. This is for the mutual protection and privacy of all staff, pupils, and parents, as well as to support data protection.

General principles for email use are as follows:
Email and Purple Mash (for homework submission) are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions).

Use of a different platform must be approved in advance by the OSL / Headteacher in advance. Any unauthorised attempt to use a different system 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).

Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL / Headteacher / DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Staff or pupil personal data should never be sent / shared / stored on email.

- If data needs to be shared with external agencies, NextCloud is available from Bedford School IT.
- Internally, staff should use the school network, including when working from home when remote access is available via Office 365 / NextCloud.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- 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 apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

13. Digital images and video

When a pupil/student 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. Parents answer as follows:

- For displays around the school
- For sticking in books as evidence of learning opportunities
- For the newsletter to illustrate an event or achievement
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

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 and surname initial if required (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Pilgrims no member of staff will ever use their personal phone to capture photos or videos of pupils unless prior permission is given by a member of the Senior Leadership Team. These will be appropriate, 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 (NB – many phones automatically back up photos). Photos are stored on the school network in line with the retention schedule of the Harpur Trust's Data Protection Policy.

The school allows parents to photograph their child using mobile phones and cameras during certain class or group performances which take place at school, such as Christmas nativity plays, music performances, Sports Day and the Year 2 performance. Parents should ask permission before taking any other photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents have no access to the school network or wireless internet on personal devices. As part of their acceptable use policy parents are reminded of the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. They are also reminded before school events.

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.

14. Personal devices including wearable technology

It is understood that staff may need to check text messages and / or personal emails in the case of an emergency or during break times. Mobile telephones must be stored in staff lockers or classroom cupboards and be switched off except during break and lunchtimes. Exceptions to this must be approved by the Headteacher/Deputy Head. Child/staff data should never be downloaded onto a private phone.

On entering the school premises, all parents and visitors are only permitted to use their phones in the main school reception area.

In the rest of the school building volunteers, contractors and governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff. Volunteers, contractors, governors can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Staff should also:

- Ensure that their own personal social networking sites are set as private and ensure that pupils are not approved contacts
- Ensure that they do not use any website or application, whether on a School or personal device, which publicly identifies their location while on School premises or otherwise in the course of their employment
- Never use or access social networking sites of pupils and not use internet or web-based communication channels to send personal messages to pupils

- Never use their own equipment (e.g. mobile telephones) to communicate with pupils - use equipment provided by the School and ensure that parents, guardians or carers have given permission
- Only make contact with pupils for professional reasons
- Recognise that text messaging should only be used as part of an agreed protocol and only when other forms of communication are not possible.

Communicating outside the agreed protocols: email or text communications between an adult and any pupil outside agreed protocols may lead to a report to external agencies in accordance with the School's child protection and safeguarding policy and procedures, disciplinary action and / or criminal investigations. This also includes communications through internet-based websites.

15. Trips / events away from school

For school trips/events away from school, teachers will contact the school office for any authorised communications with parents. If the trip is out of hours teachers may use their personal phone in an emergency but will ensure that the number is hidden to avoid a parent accessing a teacher's private phone number. Live information about school trips will be sent out via email or the relevant year group closed Facebook page.

16. Implementation, Dissemination and Review Strategies

This policy is reviewed annually by the DSL and is considered and approved by the Governing Body. It will reflect the experience and expertise of school staff, volunteers and governors.

It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups)
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Copies of this policy and supporting materials are easily accessible on the school website: **www.pilgrims-school.info**

Please note that the procedures are updated where necessary in response to developments in the school and local area. Therefore the accurate version is always the on-line version on this website.

17. Appendices

1. Acceptable Use Policies (AUPs) for:
   - KS1 Pupils
   - Staff, Volunteers & Governors
   - Visitors & Contractors
   - Parents
2. Guidance for parents about filming/photographing/streaming school events
3. Online-Safety Questions guidance for Governors (UKCIS)