Online Safety Policy

This policy applies to all pupils attending BPS. The school will ensure that all members of the school community are aware of the Acceptable Use and Online Safety policy and the implications for the individual. It should be read in conjunction with the following policies.

School Aims	Health and Safety Policy and Data Protection Policy
Safeguarding and Child Protection Policy	Positive Behaviour Policy & Anti-Bullying Policy
Acceptable Use of ICT: Pupil – Staff - Parents	PSHE Policy

Contents

Key people / dates

Designated Safeguarding Lead (DSL)	Sophie Hughes
Online-safety lead	Sophie Hughes
Link governor for safeguarding (includes online safety)	Nicola Tighe
PSHE/RSHE/RSE lead	Helen Gee / Kim Powell
Network manager / other technical support	Steve Kelly
DPO	Veritau

Policy Dissemination and Review

This policy will be available to parents via the school website and information will be shared throughout the year via the school bulletin. Staff will be familiar will the policy through termly INSET meetings as part of the safeguarding updates and in weekly briefings where necessary. This policy will be formally reviewed each year by the Online-safety Lead and updated as an ongoing process as required. The policy will be reviewed by the Governor safeguarding subcommittee on an annual basis.

Date of update	(U) Updated (R) Reviewed by	How was updated disseminated	Parents informed	Policy on website	Governor review
Sept 2016	C. Corrigan (U)	Staff briefing - email - all staff to familiarise and action	Yes	Yes	
Oct 2016	H. Gee (R)				
Feb 2017	H. Gee (U)	Staff Briefing	Yes	Yes	
Jan 2019	C. Corrigan (U)	Staff briefing – email to all staff to familiarise and action	Yes	Yes	
Jan 2020	H.Gee (U)	As above		Yes	
Jan 2021	H.Gee (R)	Teams link		Yes	
Mar2022	H. Gee (u)	Staff briefing	Yes	Yes	Yes
May 2022	H. Gee	Staff briefing & online safety training	Yes	Yes	Yes
August 22	H.Gee (u)	Email link to parents, staff briefing, INSET	Yes	Yes	Yes

Latest Updates

This year, changes to the policy particularly reflect updates in Keeping Children Safe in Education calling for greater collaboration and dialogue between safeguarding, leadership and technical teams. These include highlighting strategic responsibilities around filtering and monitoring, providing safeguarding training for *all* governors and reminders on the use of appropriate language. We also include mentions of carrying out an online safety audit (since KCSIE 2021 and still there in 2022) and online searches as part of the recruitment process (new to KCSIE 2022).

Parents must be informed about online filtering systems during periods of online learning

Parents will be made aware of the tasks pupils are asked to undertake online, what websites they may be required to access and who they are contacting from school.

Updated links, making wider use of guidance

Introduction

At BPS we believe that ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. We therefore need to build in the use of these technologies in order to provide our pupils with the skills to access lifelong learning and employment.

We are aware that raising the profile of digital learning in our school means that we must have a robust strategic plan which ensures that our pupils are able to experience all that is on offer within a safe, structured environment. This policy sets out the safety expectations of staff, parents and pupils, in respect to the use of the Internet, e-mail, messaging systems and related technologies provided by the school, and to all users accessing these services within the school environment and from home.

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 is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside your school's statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Introduction to online safety

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast passed evolution of ICT within our society as a whole as the ease of access our pupils have to ICT have outside school. Children have access to many technologies:

- Websites
- Apps
- Virtual Learning Environments
- Email
- Instant messaging and chat rooms
- Social media such as Facebook, Twitter
- Mobil/smart phones with text, video and web functionality
- Smart watches
- Other mobile devises including tablets and gaming devises
- Learning platforms and virtual learning environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video and radio/smart TV

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 is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

The main online safety risks in 2022/2023

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other aps and sites.

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.

Analysis from the Centre of Expertise on Child Sexual Abuse also highlights the prevalence of child sexual abuse, with 500,000 children estimated to experience child sexual abuse every year, whilst the Internet Watch Foundation has identified the growing risk of children, especially girls aged 11-13, targeted online by sex predators, with a three-fold increase in abuse imagery of 7–10-year-olds. This highlights transition years as crucial in the fight against sexual exploitation, in primary and secondary.

Following covid, it is important to remember more time spent online increases the risk for grooming and exploitation (CSE, CCE and radicalisation) and potentially reduces opportunities to disclose such abuse.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- 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), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

Overview

Aims

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

- Setting out expectations for all BPS community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
- 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, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- 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
- Establishing 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)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority and normally the Headmistress will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations we work with may also have advisors to offer general support. Beyond this, **click here** for a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of the BPS community (including teaching and support staff, supply teachers, governors, volunteers, contractors, pupils, parents, 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

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. Depending on their role, all members of the school community should **read the relevant section in Appendix 1** of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

Education and curriculum

We have established a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils – dedicated training around this for online safety leads is available at safetraining.lgfl.net

PSHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress." We use LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool which is linked to statements from UKCIS Education for a Connected World framework, enabling teachers to monitor progress throughout the year and drill down to school, class and pupil level to identify areas for development at **safeskillsinfo.lgfl.net**]

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

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

However, as stated in the role descriptors above, 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, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

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. We use our weekly Bulletin as a form of communication for parents to understand what systems we use to filter and monitor online use. Please see the termly curriculum maps to access details of what your children are being asked to do online. The sites they are asked to access are detailed the Pupil Planner and we will let you know if we require them to interact online with school staff.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At BPS, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are 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 (including for SEND pupils) 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.

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, PSHE/RSE and Citizenship).

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. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

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

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Positive Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly 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 on the same day – where clearly urgent, it will be made by the end of the lesson.

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

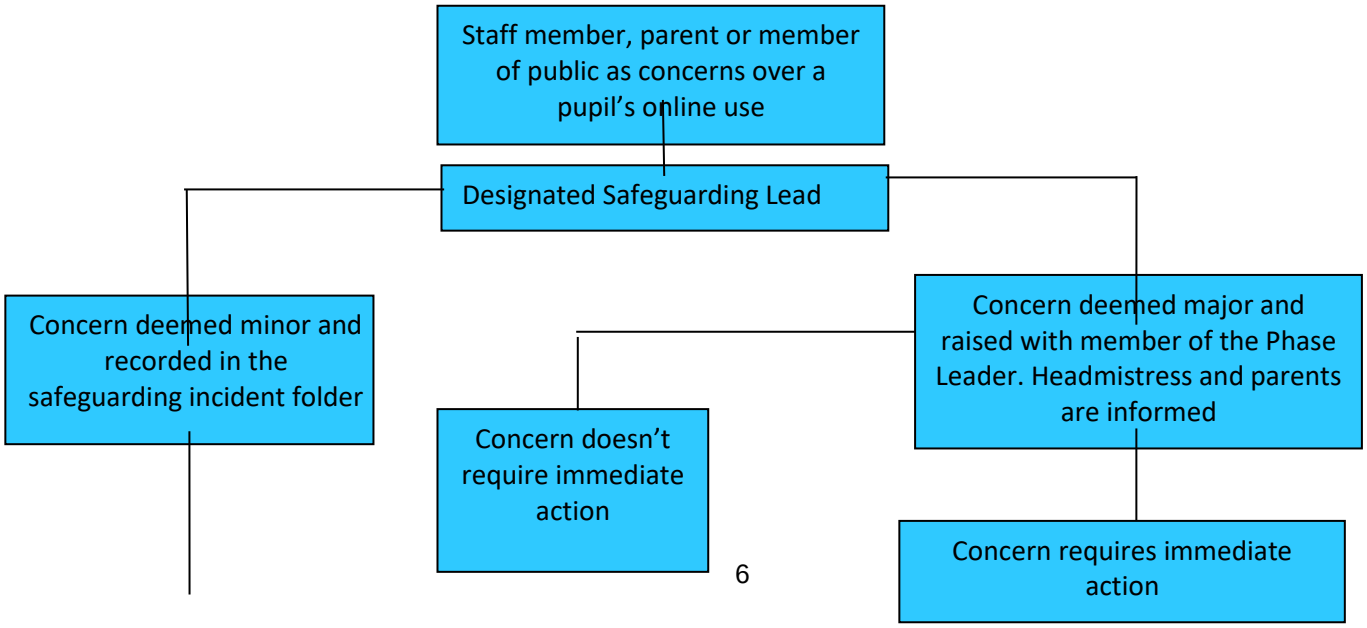
The school will actively seek support from other agencies as needed (i.e UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The new DfE guidance Behaviour in Schools, advice for Headteachers and school staff July 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

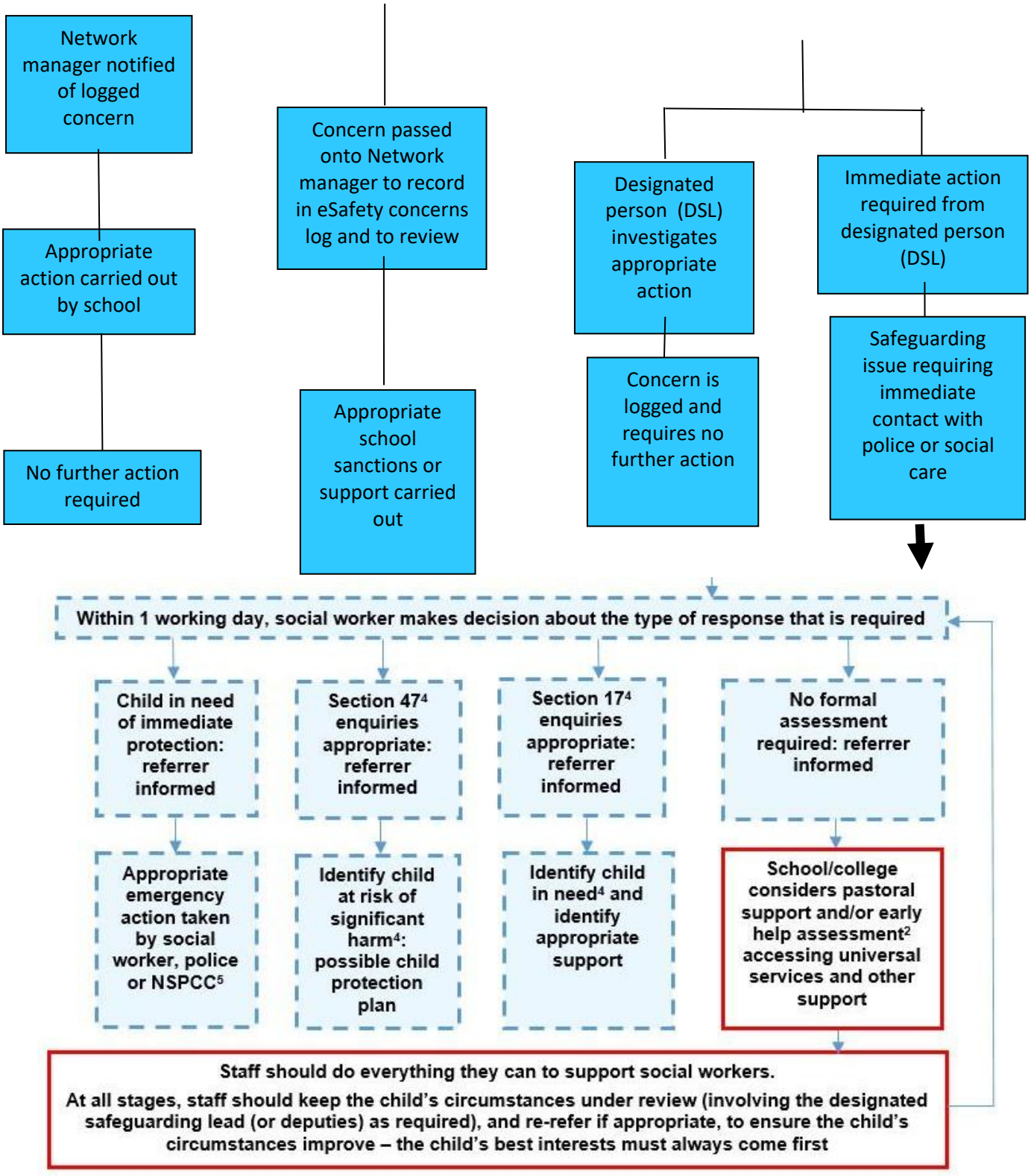
We will inform parents of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

We will evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



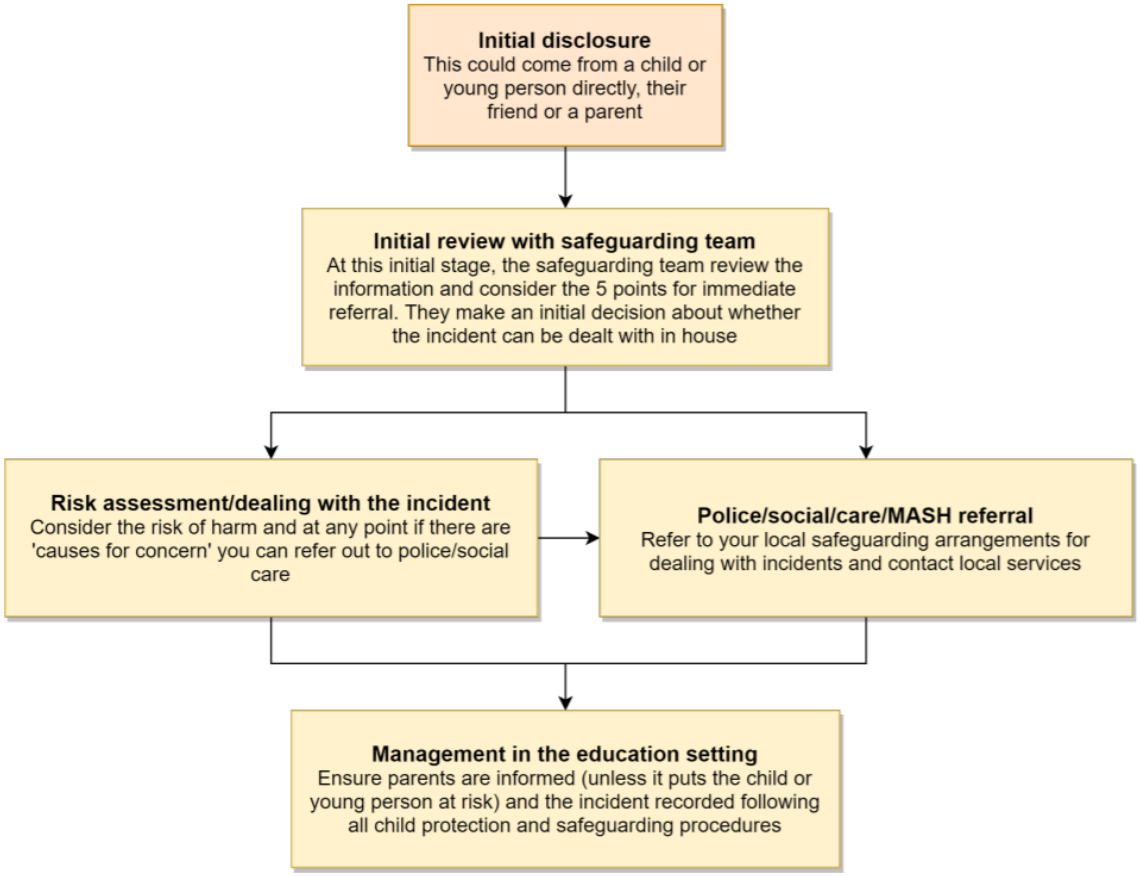


Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly 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.

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.



Consider the 5 points for immediate referral at initial review:
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

It is important that everyone understands that whilst sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting
It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

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. See our Anti-Bullying Policy
Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment
DfE guidance on sexual violence and harassment has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. All staff are made aware of this updated guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly

relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise. 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 and maintain an attitude of 'it could happen here'. 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.

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 Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy. 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. 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.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the BPS community. These are also governed by school Acceptable Use Policy and the school social media policy. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (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.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

Rigorous controls on our network, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance and Egress. The Headmistress, 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. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Additional security measures and considerations are:

- No personal devices may access school network resources
- Forced complex password and re-set periodically

- Two-factor authentication required for remote access
- Reminders to lock devices when leaving unattended
- Basic auditing facility
- Daily backups to external hard drives stored off-site
- Security processes and policies in place
- Disaster recovery policy in place
- Wireless access restricted to school-owned devices
- External file sharing of sensitive data via Egress
- Cloud platform use controlled via 2 factor authentication

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 BPS, the internet connection is provided by The 4th Utility.

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)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At BPS, we have decided that option 1 is appropriate because of the age of pupils at the school.

Electronic communications
Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy.

Email

- Pupils at BPS can only communicate to staff through the Pupil Portal
- Staff at BPS use Outlook for all school emails

Both these systems are linked to the USO authentication system and 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:

- The Pupil platform on Engage is the only means of electronic communication to be used between staff and pupils
- Email is used between staff and parents (in both directions).
- Use of a different platform must be approved in advance by the Headmistress 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 Headmistress (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 Headmistress (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, Egress systems are used.
    - Staff should use MIS, Office365 Suite (TEAMs) when working from home.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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.

See also the social media section of this policy.

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 Headmistress and Governors have delegated the

day-to-day responsibility of updating the content of the website to Gill Vasey. The site is managed and hosted InnerMedia.

The DfE has determined information which must be available on a school website.
Where other staff submit information for the website, they are asked to remember:

- 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. If in doubt, check with the Headmistress. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- 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).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service – see our DP policy here.
For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.
The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular 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
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil joins the school, parents 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 the newsletter
- 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 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 BPS, no member of staff will ever use their personal phone to capture photos or videos of pupils members of staff may occasionally use personal phones to capture photos or videos of pupils.

Photos are stored on the school network in line with the guidance for keeping and retention of information for schools. Staff and parents are reminded annually and at all school events about 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.

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 in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might

include governors, parents or younger children. Pupils are advised to be very 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

BPS's SM presence

BPS 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, and the ISI pre-inspection check includes monitoring what is being said online.

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. Sophie Hughes is responsible for managing our Twitter and Intergram accounts and checking our Wikipedia and Google reviews. S/he follows the guidance in the Safer Internet Centre online-reputation management document here.

Staff, pupils' and parents' SM presence

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 which all members of the school community sign, 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.

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).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school occasionally has to 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. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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/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. 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 (you don't need to know them – ask your child to explain it to you), 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). You may wish to refer to the new 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.

The school has an official Twitter / Instagram account (managed Sophie Hughes and will respond to general enquiries about the school, but asks parents not to use these channels to communicate about their children.
Email is the official electronic communication channel between parents and the school, and between staff and pupils.

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 pupil accounts. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headmistress, 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 Headmistress (if by a staff member).

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, bringing the school into disrepute. The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 6 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 school policy on Photography, video and video conferencing Policy and permission is sought before uploading photographs, videos or any other information about other people. The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** in Year 6 who walk to and from school unaccompanied are allowed to bring mobile phones in for emergency use only, upon arrival at school they must be handed in to the school office.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. 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.
- **Volunteers, contractors, 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 Headmistress should be sought (the Headmistress may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **Pupils** are not allowed networked file access via personal devices. However, they are allowed to access the Pupil Portal on Engage
- **Home devices** are not issued to pupils.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and Data protection and data security section. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices 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.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headmistress. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil accessing a teacher's private phone number. We use a separate protected account (class Lists) (which is private and only visible to approved members, e.g. parents) for security if we wish to give out location information, e.g. "We are all on the bus and on our way back to school now".

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headmistress 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 as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Positive Behaviour Policy.

Appendix 1 – Roles

Please read the relevant roles & responsibilities section from the following pages.
School staff – note that you may need to read two sections – if your role is reflected here, you should still read the “All Staff” section.
Roles:

- **All Staff**
- **Headmistress**
- **Designated Safeguarding Lead / Online Safety Lead**
- **Governing Body, led by Online Safety / Safeguarding Link Governor**
- **PSHE / RSE Lead/s**
- **Computing Lead**
- **Subject / aspect leaders**
- **Network Manager/technician**
- **Data Protection Officer (DPO)**
- **Volunteers and contractors (including tutor)**
- **Pupils**
- **Parents**
- **External groups including parent associations**

All staff

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL) are; notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff acceptable use policy and code of conduct
- 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, supporting curriculum/stage/subject leads, 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 and how they keep children safe).
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations infographic which applies to all online learning.
- 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 sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment (Sophie Hughes our DSL will disseminate relevant information from the updated section in KCSIE 2022 on this).
- 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 your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Headmistress

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- 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 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

- 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 remote 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. Note that KCSIE 2022 strengthens the wording for this. [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT twilight provides an overview]
- 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
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- 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 (this new addition has come into KCSIE 2022 for the first time)
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- 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

Designated Safeguarding Lead / Online Safety Lead

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"
- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
- Liaise with the Headmistress 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.
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- 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 closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school) – [see LGfL's template with questions to use at onlinesafetyaudit.lgfl.net]
- Work with the Headmistress, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net

- 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/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- 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, but also including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). 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 also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net
    - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents.

Governing Body, led by Online Safety / Safeguarding Link Governor

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated – [LGfL's Safeguarding Training for school governors is free to all governors at safetraining.lgfl.net]
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding
- 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
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Headmistress 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
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated each term in line with advice from the local safeguarding partners, integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology." [NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach]

PSHE Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. 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 [through] tests, written assignments or self evaluations, to capture progress" – [see LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net]
- This complements 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 PSHE / RSHE.
- Note that an RSHE policy should 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

Computing Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach

- Work closely with the DSL/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

Subject / aspect leaders

Key responsibilities:

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

Network Manager/technician

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. 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.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. [LGfL has a free template you can use at https://onlinesafetyaudit.lgfl.net] This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE), 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 / LGfL nominated contact / RSHE lead 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
- Maintain up-to-date documentation of the school's online security and technical procedures
- To 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, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headmistress to ensure the school website meets statutory DfE requirements

Data Protection Officer (DPO)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant

information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.

- Work with the DSL, Headmistress and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL schools for three market-leading GDPR compliance solutions at gdpr.lgfl.net
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutor)

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:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this 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 pupil AUP and encourage their children to follow it
- Talk to 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 the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

External groups including parent associations

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

Appendix 2 – Related Policies and Documents

1. Safeguarding Incident log
2. Safeguarding and Child Protection Policy
3. Behaviour Policy / Anti-Bullying Policy
4. Staff Code of Conduct
5. Acceptable Use Policies (AUPs) for:
    - Pupils Pre-Prep and Prep
    - Staff, Volunteers Governors & Contractors
    - Parents
6. Letter to parents about filming/photographing/streaming school events
7. Online-Safety Questions from the Governing Board (UKCIS)
8. Education for a Connected World cross-curricular digital resilience framework (UKCIS)
9. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
10. Working together to safeguard children (DfE)
11. Searching, screening and confiscation advice (DfE)
12. Sharing nudes and semi-nudes guidance from UKCIS:
    - *How to respond to an incident - overview for all staff
    - *Full guidance for school DSLs
    - *Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
13. Prevent Duty Guidance for Schools (DfE and Home Office documents)
14. Data protection policy
15. Cyberbullying: understand, prevent and respond (Childnet)
16. Cyberbullying: advice for headteachers and school staff (DfE)
17. Preventing and tackling bullying (DfE)
18. RAG (red-amber-green) audits for statutory requirements of school websites
19. Ofsted Review of sexual abuse in schools and colleges
20. Teaching Online Safety in School (DfE)
21. Harmful online challenges and online Hoaxes
22. Education for a Connected World (UKCIS)
23. Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
24. Indecent images of children: guidance for young people
25. Behaviour and Discipline in Schools- A guide for Headteachers and school staff
26. ISI Handbook for the Inspection of Schools - Commentary on the Regulatory Requirements
27. Keeping children safe in education; Statutory guidance for schools and colleges; September 2022
28. Communications Act 2003
29. Computer Misuse Act 1990
30. Human Rights Act 1998
31. Malicious Communications Act 1988:
32. Telecommunications Act 1984:
33. Copyright, Designs and Patents Act 1988
34. The Data Protection Act 2018:
35. UK General Data Protection Regulation (UK GDPR):
36. Obscene Publications Act 1959 and 1964
37. Protection of Children Act 1978:
38. Protection from Harassment Sct 1997:
39. Public Order Act 1986:
40. Racial and religious hatred Act 2006:
41. Sexual Offences Act 2003:
42. Equality ct 2010:

Appendix 3

Measures Taken

We have created a safe digital learning environment consisting of the following elements:

- Web Filtering - Web filtering is handled by our firewall, it detects the user or device that is logged in and applies the appropriate level of filtering. The categories that are blocked are discussed with the SLT

- Web Monitoring – Pupils are not allowed to access IT equipment without there being a member of staff present

- Safesearch - Safesearch facilities have been enabled for the major search engines and streaming media sites where possible. SSL (Secure Sockets Layer) Inspection is also enforced for pupil traffic which allows secure content to be inspected to detect search terms.

- Port and Service Restrictions - Access has been given to only essential ports and services through the firewall.

- Mobile Device Management (MDM) – whilst no MDM software is deployed network level filtering is applied and is not reliant on any software on user devices whilst at school. Staff devices may have be used to work from home, but are never accessed by pupils.

Appendix 4

Websites for Pupils and Parents

KidSmart - Learn more about the Internet and how to be a SMART surfer

ThinkUKnow - Advice on online safety

CBBC Stay Safe - ESafety games and songs

Childnet - Working to make the Internet a safe place for children

DigiDuck's Big Decision - A story about online friendship and making the right decisions (KS1)

Adventures of Smartie The Penguin -A story about asking for help when using the Internet (KS1)

Digizen - Become a responsible digital citizen

The Adventures of Kara, Winston and the SMART Crew

Safe Network - Guidance on helping keep children safe online

The Parents' and Carers' guide to using the Internet

CEOP YouTube Channel (for Parents/Carers)

Digital Family - o2

Keep Safe Online - Cyberbullying

Keep Safe Online - Glossary of Terms

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  o ChildLine: www.childline.org.uk
  o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Telephone helpline: 0844 381 4772

Appendix 5

Keeping children safe when accessing remote learning

Whilst we are still living with COVID-19, it is important that we follow any current government guidance should we face any future school closures. This Appendix sits alongside the School's existing Safeguarding Policy and will apply when the School is not in session or when children are working remotely.

This policy complies with the following key documents:

- Guidance for full reopening of schools (HM Government, July 2020 onwards)
- Safeguarding and remote education during coronavirus (COVID-19) (HM Government, April 2020) Principles

As far as is reasonably possible, we will take a whole institution approach to safeguarding. This will allow us to satisfy ourselves that any new policies and processes in response to COVID-19 are not weakening our approach to safeguarding or undermining our Safeguarding Policy. Whilst the way that we operate in response to COVID-19 is fundamentally different to business as usual, a number of important safeguarding principles remain the same:

The best interests of children will always continue to come first.

If anyone has a safeguarding concern about any child then they should continue to act and to act immediately.
A DSL or a DDSL will always be available and members of the SLT can continue to be consulted as and where necessary.

It is essential that unsuitable people are not allowed to enter the children's workforce and / or gain access to children, which means that Safer Recruitment principles remain in place.

Children should continue to be protected when they are online.

This Appendix to the School's Online Safety Policy contains details of our arrangements keeping children safe.

Additional risks

The risks which are present in a physical setting are, by and large, equally present in a virtual setting.

There are also added risks including the particular emotional vulnerability of children in a time of crisis; concern about family members and friends; the potential for increased power imbalance; and the potential for neglect within the family for reasons of illness, anxiety or work requirements. Above all, the uniqueness of the situation why children may be working remotely with the potential informality of virtual learning may unwittingly facilitate culture slippage, where rules which are routinely applied in ordinary circumstances are seen to be irrelevant in a crisis or in the case of unusual events. Additional safeguarding risks relating to online learning may arise due to poor technical understanding; an intention to abuse; weak online security, poor parental settings on home systems; and patchy parental supervision. Also, there is greater likelihood of Youth Produced Sexual Imagery (sexting), and neglect to children where parents are ill, anxious, or busy at work.

Contact details

In the event of remote learning the Safeguarding Team and SLT continue to remain available so as to be able to receive and respond to any concerns that might arise. This can be done by email, telephone or video call. The Safeguarding Team continues to work alongside Children's Services and the LADO. All members of the Safeguarding Team have access to the School site and any relevant files and documentation, should the need arise.

Vulnerable children

Vulnerable children include those who have a social worker with education, health and care (EHC) plans. Those who have a social worker include children who are subject to a Child Protection Plan, a Child in Need Plan and those who are looked after by the Local Authority. We will continue to work with and support children's social workers to help protect vulnerable children.

The Headmistress, DSL and DDSLs know who all our vulnerable children are: they also have the flexibility to offer support to those on the edge of receiving children's social care support. The school expects all pupils to attend the school remotely and, where it is deemed to be appropriate, will encourage parents of our vulnerable children to allow them to attend physically. If the expectation is that a vulnerable pupil will attend the school physically, consideration will be given as to whether the pupil has any underlying health conditions that put them at risk and will be subject to the formal agreement with the child's social worker. In circumstances where a parent does not want to bring their child to an education setting, and their child is considered vulnerable, the social worker and the school will explore the reasons for this directly with the parent following the advice set out by Public Health England.

The School will ensure that all professionals (e.g. social workers, SEND case workers, Early Help worker etc.) involved with these vulnerable children are fully informed around the current attendance of the child (attending School or not, either remotely or physically) and if not attending School, the arrangements that have been put in place around safeguarding the child.

Registration and attendance

The School will continue to record day-to-day attendance. Absences will be reported as is usual and any unexplained absences will be followed up. Vulnerable children who are required to attend school every day whether physically or

virtually (including Looked After Children, Children subject to a Child Protection Plan and Children subject to a Child in Need Plan) and who are absent, will result in the school contacting the relevant Children's Services and providing the following details:

- School name and DSL details
- Full name of child
- Date of birth of child
- When the child was last seen by school staff

Staff absence

If a member of staff is ill and needs to be absent for a school session, the line manager should be notified by 08h30; for teaching staff, the Head's PA and school secretary should also be informed. If there is to be a planned absence, authorisation should be sought by completing the relevant absence request form or by email. These arrangements ensure that pupils can be properly registered and supervised.

Reporting a concern

Where staff have a concern about a child, they should continue to follow the process outlined in the school's Safeguarding Policy. Where staff are concerned about an adult working with children in the school, they should continue to follow the normal procedures and notify the Headmistress immediately or the Chair of Governors if the matter concerns the Headmistress. If there is an immediate concern or the relevant person is not available, then it is appropriate to contact the Local Authority and / or the Police.

Safeguarding training

All staff have had safeguarding training and have read Part 1 of Keeping Children Safe in Education (2022). The DSL will continue to keep staff updated regarding safeguarding updates via CPS sessions or the weekly staff briefing so that they know what to do if they are worried about a child. Where there is an update to the school's Safeguarding Policy, it will be necessary for all members of staff to confirm that they have read and understood the school's revised Safeguarding Policy.

Where new staff are recruited, or new volunteers enter the school, they will continue to be provided with a safeguarding induction, and may be provided online or face-to-face. If the need arises for staff to be deployed from another education or children's workforce setting, the school will take into account the DfE supplementary guidance on safeguarding children during a pandemic and will accept portability as long as the current employer confirms in writing that:

- The individual has been subject to an enhanced DBS and children's barred list check
- There are no known concerns about the individual's suitability to work with children
- There is no ongoing disciplinary investigation relating to that individual. Upon arrival, they will be given a copy of the school's Safeguarding Policy, confirmation of local processes and confirmation of DSL arrangements.

Safer recruitment / volunteers

It remains essential that people who are unsuitable are not allowed to enter the children's workforce or gain access to children. When recruiting new staff, the school will continue to follow the relevant safer recruitment processes for their setting, including, as appropriate, relevant sections in Part 3 of Keeping Children Safe in Education (2022) (KCSIE).

Where volunteers are deployed, the school will continue to follow the checking and risk assessment process as set out in the relevant sections of KCSIE (2022). Under no circumstances will a volunteer who has not been checked be left unsupervised or allowed to work in regulated activity. The school will continue to follow its legal duty to refer to the DBS where appropriate, in line with advice from the LADO, anyone who has harmed or poses a risk of harm to a child or vulnerable adult.

The school will continue to consider and make referrals to the Teaching Regulation Agency (TRA) as set out in the relevant section of KCSIE (2022) and the TRA's "Teacher misconduct advice for making a referral".

Whilst acknowledging the challenge of a national emergency, it is essential from a safeguarding perspective that the School is aware, on any given day, which staff / volunteers will be in school, and that appropriate checks have been carried out, especially for anyone engaging in regulated activity. As such, the school will continue to keep the single central record (SCR) up to date as outlined in the relevant section of KCSIE. The SCR can also be used to log details of any risk assessments carried out on volunteers.

Online safety through school systems and in school

The school will continue to provide a safe environment, including when working online. This includes the use of appropriate filters and online monitoring systems applied to the school's online platforms, through which all school business must be conducted. Where children are using computers in school, appropriate supervision will be in place. The school will ensure that any use of online learning tools and systems is in line with privacy and GDPR requirements.

Online safety away from school

It is important that all staff who interact with children, including online, continue to look out for signs that a child may be at risk. To report any such concerns, staff should continue to follow the process outlined in the School's Safeguarding Policy; where appropriate, referrals should still be made to Children's Services and, as required, the Police.
Pupils will be briefed on how to keep themselves safe when online, reporting matters to members of staff or using the following websites:

- Childline for support: https://www.childline.org.uk/
- UK Safer Internet Centre to report and remove harmful online content: https://reportharmfulcontent.com/

- CEOP for advice on making a report about online abuse: https://www.ceop.police.uk/safety-centre/

The Headmistress leads on matters related to remote teaching and the school's Remote Learning Procedure gives clear advice and guidance. The following expectations are to be observed when engaging in virtual lessons and especially where webcams are involved.

Appearance and presentation

- Pupils should have a workspace that is quiet, safe and free from distractions.
- Pupils should work from a computer that has a strong internet connection and videoconferencing functionality.
- Any computers used should be in appropriate professional spaces (for example, not in bathrooms).
- When video-calling on Zoom/TEAMs, pupils and staff should select an appropriate professional background to ensure privacy. Video backgrounds are not permitted.
- Staff and pupils must wear appropriate clothing for video-calls, as should anyone else in the household who might be visible. Other than the staff and the pupil, no other member of the household should be in attendance during lessons, except by prior arrangement and with the explicit permission of all parties.

Scheduling and different types of meeting/learning sessions

Staff and pupils should adhere to the published timetable for lessons and events. Small group meetings are to be preferred to one-to-one meetings.

Where one to one sessions need to be scheduled, they should be pre-arranged as a calendared meeting, at a mutually convenient time during the conventional working day.

If either a pupil or a member of staff has a concern about the nature of any online interaction, the matter should be reported to the DSL.

Video calling and online platforms

- Live classes and images through the online platforms are not to be recorded, except with the explicit permission of all relevant parties and only for the purposes of examination assessment.
- All participants in any online video call should be visible except when specifically instructed that video should be disabled.
- Only platforms provided by the school should be used in order to communicate between members of staff and pupils.
- Any behaviour or comments that are inappropriate should be reported to the Phase Leader, or, in the case of a safeguarding concern, to the DSL.

Expectations of households where pupils are working

Pupils need to be able to work in a workspace that is quiet, safe and free from distractions. Pupils will need access to a computer that has wireless access and video-conferencing facilities. It is not expected that other members of the household will be in attendance or take part in a scheduled session with a member of staff, unless a separate meeting has been specifically arranged. It is not appropriate for parents to record, share or comment in any public or closed forum about individual pupils or members of staff.

Supporting children when they are not in school

Physical wellbeing

Protracted periods of time sat in front of a computer are not healthy. All members of the community should seek to break up their screen-time, taking breaks regularly away from the screen.

Pupils on the edge of social care support

The school is committed to ensuring the safety and wellbeing of all of its pupils. Where the DSL has identified a pupil to be on the edge of social care support, or who would normally receive enhanced levels of pastoral-type support in school, Phase Leaders in discussion with the DSL will ensure that a robust communication plan is in place for that child. The communication plan could include: strategic remote contact, telephone contact and door-step visits.

Emotional welfare

The school recognises that it has a role to play in protecting the welfare of its pupils and recognise that the impact of remote learning can affect the mental health of pupils, their parents / guardians and their families. Staff need to be aware of this in setting expectations of pupils' work and of the way in which they interact with pupils and their families.

Child-on-child abuse

Where the school receives a report of child-on-child abuse, the principles as set out in KCSIE (2022) and those outlined within the school's Safeguarding Policy will be followed. The school will listen and work with the child, parents and any multi-agency partner required to ensure the safety and security of that young person. Concerns and actions must be recorded via CPOMs, and appropriate referrals made.

Move to top of document