




Online Safety Policy

Ratified by Governors: 6 July 2022
Review Date: May 2023
Member of Staff Responsible: F Singh

Introduction

Key people / dates

 <p>Bush Hill Park Primary School</p>	Designated Safeguarding Lead (DSL)	Anastasia Neocleous
	Online-safety coordinator (if different)	Fateh Singh
	Online-safety / safeguarding link governor	Rachael Sitch
	PSHE lead	Anastasia Neocleous
	Network manager / other technical support	Fateh Singh
	Date this policy was reviewed and by whom	Fateh Singh, April 2022
	Date of next review and by whom	Fateh Singh, May 2023

Contents

Introduction.....	2
Key people / dates.....	2
Contents	2
Overview.....	4
Aims	4
Further Help and Support.....	4
Scope	4
Roles and responsibilities	4
Headteacher – Anna Theodosiou	5
Online Safety Lead – Fateh Singh	6
Governing Body, led by Safeguarding Link Governor – Rachael Sitch.....	8
All staff.....	9
PSHE LEAD – Anastasia Neocleous	10
Computing Curriculum Lead – Fateh Singh	10
Subject leaders	10
Network Manager – Fateh Singh	10
Data Protection Officer in school (DPO) – Lorraine Shaw	11
LGfL TRUSTnet Nominated contacts – Fateh Singh.....	11
Volunteers and contractors.....	12
Pupils	12

Parents/carers	12
External groups including parent associations – FOBHPS	12
Education and curriculum.....	13
Handling online-safety concerns and incidents.....	14
Actions where there are concerns about a child.....	15
Sexting – sharing nudes and semi-nudes	16
Bullying	17
Upskirting.....	17
Sexual violence and harassment	17
Misuse of school technology (devices, systems, networks or platforms).....	17
Social media incidents	17
Data protection and data security.....	18
Appropriate filtering and monitoring	19
Electronic communication.....	19
Email	19
School website.....	20
Cloud platform.....	20
Digital images and video.....	20
Social media.....	21
Staff, pupils’ and parents’ SM presence.....	22
Device usage.....	23
Personal devices including wearable technology.....	23
Network / internet access on school devices.....	23
Trips / events away from school.....	23
Searching and confiscation.....	24
Safeguarding & Online Safety Policy / AUP Addendum for Home Learning during Closures	25
Appendices	26

Overview

Aims

This policy aims to:

- Set out expectations for all Bush Hill Park Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help 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
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour for learning or Safe to learn 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 our Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority supports organisations we work with and also have advisors to offer general support.

Beyond this, [reporting.lgfl.net](https://www.reporting.lgfl.net) has 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 Whistleblowing Helpline, as well as hotlines for hate crime, terrorism, fraud and anonymous support for children and young people.

Scope

This policy applies to all members of the Bush Hill Park Primary School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Roles and responsibilities

This school is a community school and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher – Anna Theodosiou

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed and adhered to by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance
- 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
- 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
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

Online Safety Lead – Fateh Singh

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 2021 and updated version from Sept 2022):

- “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 (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.)
- 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 approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- “Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.”
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, 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.
- 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 is 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). To use LGfL filtering, view the appropriate filtering statement here. Talk to our technical teams. Whilst they will do the technical work, key decisions on what should be allowed are the responsibility of the DSL who should be careful to keep children safe but “be careful that ‘over blocking’ does not lead to unreasonable restrictions” (KCSIE). Our Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview.
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
 - All staff must read KCSIE Part 1 and all those working with children
 - it would also be advisable for all staff to be aware of Annex C (online safety)
 - cascade knowledge of risks and opportunities throughout the school

- Pay particular attention to online tutors this year, 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 - share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles.

Governing Body, led by Safeguarding Link Governor – Rachael Sitch

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) and that the DSL has the appropriate status and authority, 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 co-ordinator / 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 headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in the school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and are regularly updated in line with advice from the LSCB. Online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
- Ensure appropriate filters and appropriate monitoring systems are in place and be careful that 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL – Anastasia Neocleous) and Online Safety Lead (OSL – Fateh Singh)
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, 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, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE LEAD – Anastasia Neocleous

- 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
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

Computing Curriculum Lead – Fateh Singh

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 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 leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, 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 our 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 – Fateh Singh

Key responsibilities:

- As listed in the 'all staff' section, plus:
- 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 TRUSTnet nominated contact to ensure that school systems and networks reflect school policy

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school’s online security and technical procedures
- 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
- Network managers/technicians at LGfL TRUSTnet schools may want to ensure that we take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish (from Sept 2018), Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress (from Sept 2018), Meraki Mobile Device Management and CloudReady/NeverWare. These solutions which are part of the school’s package will help protect the network and users on it
- 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 Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer in school (DPO) – Lorraine Shaw

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’ (April 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.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and monitored and audited

LGfL TRUSTnet Nominated contacts – Fateh Singh

Key responsibilities:

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant

- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- 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
- 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
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible 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.
- NB: the LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety (but only half talk about it with them more than once a year).

External groups including parent associations – FOBHPS

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

Education and curriculum

The following subjects have the clearest online safety links:

- PSHE
- Health Education, Relationships (in secondaries: Relationships and Sex) Education (being implemented from September 2019 for September 2020)
- 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/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Bush Hill Park Primary School, 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' from UKCCIS (the UK Council for Child Internet Safety, soon to become UKCIS, no longer solely for children).

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, Citizenship and (from September 2019 for September 2020) the new statutory Health Education and Relationships Education).

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.

Non-teaching 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
- Sexual Harassment / Peer on Peer Abuse Policy (if separate)
- Safe to learn Policy
- Behaviour for learning Policy
- Acceptable Use Policies
- Prevent Policy
- 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 on pupils when they come into 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.

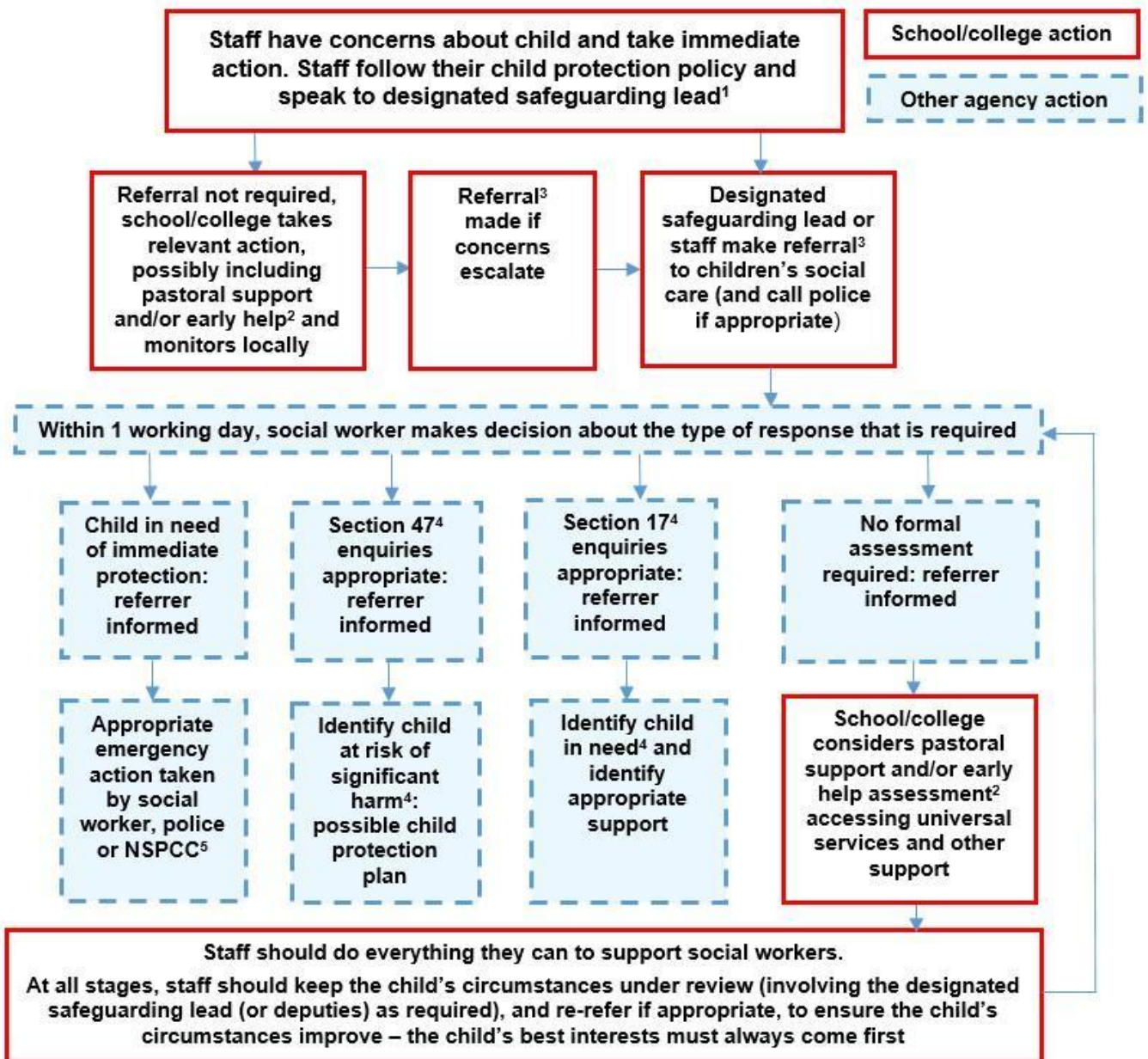
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

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

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

Actions where there are concerns about a child

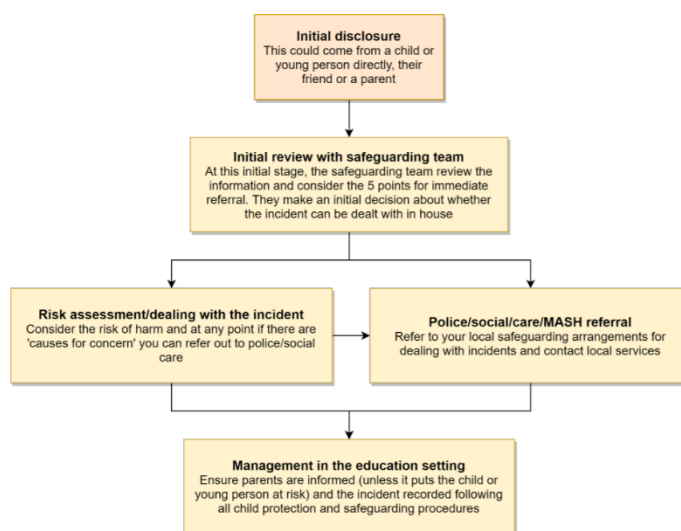
The following flow chart is taken from page 22 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



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 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.



*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/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 should be treated like any other form of bullying and the school Safe to learn policy should be followed for online bullying, which may also be referred to as cyberbullying.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. All staff will be made aware of this guidance: paragraphs 45-49 cover the immediate response to a report 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 will work to foster a zero-tolerance culture. The school will 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.

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

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/handbook.

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 Bush Hill Park School community. These are also governed by school Acceptable Use Policies.

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, Bush Hill Park 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 (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal 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. 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. As with all data sharing, **appropriate organisational and technical safeguards should still be in place.** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.”**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found here. <http://www.bushhillpark.enfield.sch.uk/school-information/policies>
Further, this school makes use of the following discounted GDPR solution from LGfL TRUSTnet:

- GDPR.co.uk from Wonde

Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, 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: USO sign on for LGfL TRUSTnet services, Sophos Anti-Virus, Sophos Anti-Phish*, Sophos InterceptX, Sophos Server Advance, Egress*, Meraki Mobile Device Management and CloudReady/NeverWare.

* from Sept 2018

The headteacher, 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 USO-FX and 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.

Appropriate filtering and monitoring

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

At this school, the internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools.

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

Electronic communication

Email

- Pupils at this school use the LondonMail / PupilMail LGfL TRUSTnet for all school emails and Google classroom and Microsoft 365 systems
- Staff and Governors at this school use Office 365 for all school emails

All these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL TRUSTnet on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support GDPR

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately. Staff or pupil personal data should never be sent/shared/stored on email.
 - If data needs to be shared with external agencies, USO-FX and Egress (from Sept 2018) systems are available from LGfL TRUSTnet.
 - Internally, staff should use the school network, including when working from home when remote access is available via the RAV3 system.
- Pupils in Key Stage 2 are restricted to emailing within the school and cannot email external accounts
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils, staff and Governors are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Fateh Singh. The site is managed by / hosted by WebyAnywhere.

The Department for Education has determined information which must be available on a school website. LGfL TRUSTnet has compiled RAG (red-amber-green) audits to help schools to ensure that requirements are met.

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. Sources must always be credited and material only used with permission. If in doubt, check with Fateh Singh. There are many open-access libraries of high-quality public-domain images that can be used. Pupils and staff at LGfL TRUSTnet schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net

Cloud platform

This school adheres to the principles of the Department for Education document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)'

- 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
- Username and password 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

Digital images and video

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

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 Bush Hill Park Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on the school network in line with the retention schedule of the school GDPR procedures.

Staff and parents are reminded annually 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), GDPR, 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.

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 are subject to bullying or abuse.

Social media

Bush Hill Park Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

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.

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 (which can be found via <http://www.bushhillpark.enfield.sch.uk/school-information/policies>) 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, but the school regularly deals with issues arising on social media with pupils/students 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 following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent 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, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The school has an official Twitter account (managed by the headship team) and will not respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children. If parents/carers have a query, please contact the school office.

Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils/students 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/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

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

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

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online.

They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute.

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 Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

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

- **Pupils/students** who do bring in a mobile phone/smart watch/other recordable digital devices must hand in their device to the school office for safe keeping. Under no circumstances must pupils use their mobile phone during the school day.
- **All staff who work directly with children** should leave their mobile phone/smart watch/other recordable digital devices 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 headteacher should be sought (the headteacher 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.

Network / internet access on school devices

- **Pupils/students** are not allowed networked/wireless file access via personal devices.
- **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.
- **Volunteers, contractors, governors** access the wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored/restricted.
- **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/students 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 headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher 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.

Safeguarding & Online Safety Policy / AUP Addendum for Home Learning during Closures

During school closures and remote learning, the same principles of safeguarding, online safety and behaviour apply – major changes to policy documents should not be needed. However, all policies are being reviewed, are reminding stakeholders of existing principles and identifying any which need reinforcing due to new (mostly online) procedures and activities.

1. The new DfE Covid Safeguarding Guidance is essential reading you can read this guidance here: safepolicies.lgfl.net.
2. There are many online scams playing on people's fears and the current situation. See coronavirus.lgfl.net/security for help keeping staff and families safe & secure (including staff training).
3. All policy and AUP issues are worthy of reminders, but especially the importance of critical thinking: not just to combat fake news and scams, but also because of increased grooming activity relating to radicalisation or child sexual exploitation as a result of greater online access to children.
4. 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.
5. See infographic and further information safeguarding principles for remote lesson - <https://remotesafe.lgfl.net/> additional the school website contains additional information for parents and carers - <https://www.bushhillpark.enfield.sch.uk/curriculum/remote-learning>
6. We are encouraging parents to keep children safe with regular correspondence. More resources can be found at: parentsafe.lgfl.net
7. In school we have 'appropriate filtering' but at home many parents will not be using parental controls, so we will remind them to do so (Internet Matters has guides). Now is also a good time to promote child-safe search engines e.g. [swiggle.org.uk](https://www.swiggle.org.uk) and YouTube Kids instead of YouTube.
8. Lots of people are offering their services on social media to give online tuition to other people's children. We will remind parents not to engage someone they do not know, that they should listen in where possible, any sessions should be in family areas not bedrooms, and that children need to be told that tutors should not arrange new sessions or online chats directly with them.
9. Any issues relating to online/offline can be brought to the attention of our achievements leads, senior leaderships team and/or other staff. We continue to use our systems for logging concerns.

Appendices

1. Acceptable Use Policies (AUPs) for:
 - o Pupils (Key Stage 2)

Our agreement

Our school policy

Teacher's agreement
I agree to monitor and review pupils internet access within the school and to support pupils who report anything that makes them feel uncomfortable.
Signed: *Fsingh* (Mr. F Singh)

Parent/Carer's agreement
I give permission for access to the Internet on the terms set out in the schools internet access policy.
Signed:

Pupil's agreement
I agree to follow the rules for safe use of the school's computer system.
Signed:

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.

The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.

Neither the school nor the London Borough of Enfield can accept liability for the material accessed, or of any consequences thereof.

Student Code of conduct

Policy for Safe use of the school's computer system – please find information about our schools policy and some useful links.

Bush Hill Park Primary School

Childnet International **LONDON** **UK Safer Internet Centre**

I will keep my school safe

- ✓ I will only access the system with my class login.
- ✓ I will only use the computers for school work and homework.
- ✓ I will not bring Mobile phones, USB keys, MP3 players, hand held games devices or other removable media into school unless I have been given permission.



I will be fair to others

- ✓ I will only email people I know, or my teacher has approved. The messages I send will be polite and sensible.
- ✓ I will not access other people's files. I will always ask permission before printing.
- ✓ I understand that the school may check my computer files and may monitor the Internet sites I visit.
- ✓ I will not post inappropriate messages or images about others on ANY form of social media..



I will keep myself safe

- ✓ I will ask permission from a member of staff before using the Internet.
- ✓ I will not give my home details or arrange to meet someone unless my parent, carer or teacher has given permission.
- ✓ To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
- ✓ I will keep my personal login details safe and not share them with others.



The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

What is an AUP?

We ask all children, young people and adults involved in the life of Bush Hill Park Primary School to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy - <http://www.bushhillpark.enfield.sch.uk/downloadfile/5106191>

Where can I find out more? All staff, governors and volunteers should read Bush Hill Park Primary School's full Online Safety Policy (link above) for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Mr F Singh (helpdesk@bushhillpark.enfield.sch.uk).

What am I agreeing to?

1. (This point for staff and governors): I have read and understood Bush Hill Park Primary School's full Online Safety policy <http://www.bushhillpark.enfield.sch.uk/downloadfile/5106191> and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead - Mrs Anastasia Neocleous.
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my 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.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same.

7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession), and I will do nothing to impair either.
9. I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
10. I agree to adhere to all provisions of the General Data Protection Regulation (GDPR) at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, log off devices when unattended to protect data, never share credentials and immediately change passwords and notify Mr F Singh if I suspect a breach. I will not store school-related data on personal devices, personal storage i.e. USB keys or cloud platforms.
11. I will not copy and paste confidential files relating to staff or pupils on the desktop of class room or office based PCs, laptops or any other devices, ensuring data is protected and only used in the way that it was intended and is only accessible to staff members authorised to do so.
12. I understand that I should only allow pupils to use devices specifically for pupil use.
13. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use".
14. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
15. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
16. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture, but only if I tell somebody. I have read the sections on handling incidents and concerns about a child in general, sexting, bullying, sexual violence and harassment, misuse of technology and social media.
17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature:

Name:

Role:

Date:

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature:



Name:

Headteacher

Role:

Mrs Anna Theodosiou
