Bishop Perrin
Church of England Primary School

Online Safety Policy

Non-statutory Policy
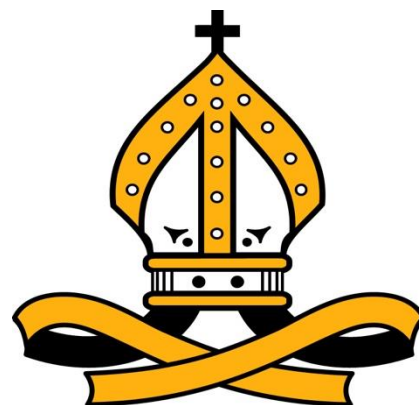
Designated Safeguarding Lead (DSL) and Deputy DSL	Mary McAvoy (DSL) and Rachael Macklearn (DDSL)
Online-safety Lead	Mary McAvoy
Curriculum Computing Lead	Rachel Lawrence
PSHE and RSE Lead	Amanda Crinall
Safeguarding Governor	Mrs Lucy James
Web Filtering Governor	TBC
Network Manager	Click On It London (0345 094 1005)
Policy author	Adrian Corke
Ratification level	Full Governing Board
Date this policy was reviewed	Sept 2023
Policy renewal date (unless changes occur)	Sept 2025
Frequency of review	Bi-annually

This policy is part of the School's statutory Child Protection and Safeguarding Policy. Any issues and concerns with online safety <u>must</u> follow the school's safeguarding and child protection processes.

CONTENTS

1   WHAT IS THIS POLICY?

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' (KCSiE), 'Teaching Online Safety in Schools' and other statutory documents. It complements existing subjects including; Relationships and Sex Education (RSE), PSHE and Computing; it is designed to sit alongside our school's statutory Child Protection and Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

2   HOW WILL THIS POLICY BE COMMUNICATED?

This policy will communicated to the school community in the following ways:
- The school website
- Available on request in paper format from the School Office
- Available on the internal staff network
- Available in paper format in the Planning, Preparation and Assessment Room
- As part of the school induction pack for all new staff
- Referenced in the Staff Handbook
- As part of the range of key policies that staff read and sign against annually to say that they have understood and will abide by them
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, Governors, pupils and parents/carers (Parents are asked to abide and support the Parent/Carer AUP by acknowledging it on the annually updated Pupil Emergency Contact Form)
- AUPs are displayed in classrooms and are available on the school website

3   AIMS

This policy aims to:
- Set out expectations for all of Bishop Perrin School's 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
- 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 and 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 Policy or Anti-Bullying Policy).

4   FURTHER HELP AND SUPPORT

The school will follow guidance as laid out in the DfE's [Teaching Online Safety In School](#). School procedures 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 the school's Child Protection and Safeguarding Policy. The DSL/DDSL will handle referrals to Richmond Council's Single Point of Access (SPA) and the Headteacher will handle referrals to the Local Authority Designated Officer (LADO).

Beyond this, [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 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. Training is also available via [safetraining.lgfl.net](#)

5   SCOPE

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

6   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. The school community have a responsibility 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. ALL school staff must ensure that they have fully read, understand and will abide by the responsibilities laid out in Section 10 of this policy.

From September 2023, it is vital that all members of staff understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

7   HEADTEACHER

Key responsibilities:
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the DSL and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (see LGfL's template with suggested questions at onlinesafetyaudit.lgfl.net)
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information, ensuring the responsibilities of the DSL are being followed and fully supported
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Kingston and Richmond Safeguarding Children Partners (SCP) guidance
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the Data Protection Officer (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
- 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
- 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
- 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
- Have an understanding and review, along with the school's IT technicians, the DSL and Web Filtering Governor, the school's systems for filtering and monitoring use of the school's internet and the devices that are using it. This understanding also includes knowing what is blocked or allowed for whom, when, and how as per KCSIE. KCSIE Webfiltering | LGFL
- In consultation with the DSL, the school's IT technicians and the Web Filtering Governor, undertake regular filtering and monitoring checks of the school's internet usage and report to the Governing Board. LGfL's Safeguarding Shorts: Filtering for DSLs and SLT
- Ensure all Governors 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. LGfL's Safeguarding Training for School Governors is free to all governors at safetraining.lgfl.net
- Ensure the school website meets statutory DfE requirements: websiterag.lgfl.net (see appendices for website audit document)

8   DESIGNATED SAFEGUARDING LEAD / ONLINE SAFETY LEAD

Key responsibilities

"The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety **and understanding the filtering and monitoring** systems and processes in place) … this lead responsibility should not be delegated" Keeping Children Safe in Education 2021.

- Where the Online Safety Lead is not the named DSL or DDSL, 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 ALL staff undergo safeguarding and child protection training (including online safety which incorporates filtering and monitoring guidance) at induction and that this is regularly updated safecpd.lgfl.net
- Liaise with the Headteacher and Chair of Governors to ensure that ALL Governors 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
- Ensure an effective approach to online safety that enables 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.
- Take lead responsibility for webfiltering and monitoring of the school's internet usage and systems
- Have an understanding and review, along with the school's IT technicians, the Headteacher and Web Filtering Governor, the school's systems for filtering and monitoring use of the school's internet and the devices that are using it. This understanding also includes knowing what is blocked or allowed for whom, when, and how as per KCSIE. KCSIE Webfiltering | LGFL
- In consultation with the Headteacher, IT technicians and the Web Filtering Governor, undertake regular filtering and monitoring checks of the school's internet usage and report to the Governing Board. In doing so, review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping LGfL's Safeguarding Shorts: Filtering for DSLs and SLT
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)
- Work with the 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 developments in online safety and undertake PREVENT awareness training prevent.lgfl.net
- Review and update this policy, Acceptable Use Policies and the strategy on which they are based
- Receive regular updates in online safety issues and legislation and be aware of local trends LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents parentsafe.lgfl.net

- 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 staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including Harmful Sexual Behaviours and bullying).

9 SAFEGUARDING GOVERNOR

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions from the UK Council for Child Internet Safety (UKCCIS) 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) with the appropriate status and authority and time, funding, training, resources and support.
- Undergo (and signpost all other Governors) 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. Free Governor safeguarding training: safetraining.lgfl.net
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Appoint a Web Filtering Governor to work closely with the DSL on filtering and monitoring standards at the school. Guidance can be sought from: safefiltering.lgfl.net
- Ensure appropriate filters and appropriate monitoring systems are in place, ensuring "overblocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding
- Have regular strategic reviews, incorporating discussions about filtering. Monitoring and blocking, with the Online Safety Lead/DSL and incorporate online safety into standing discussions of safeguarding at Governor meetings
- Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure that all staff undergo safeguarding and child protection training (including online safety and monitoring and filtering) at induction and that it is regularly updated. Online safety training for staff can be accessed: cpd.lgfl.net
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

10 ALL STAFF

Key responsibilities:

- Read and follow this policy in conjunction with the school's main Child Protection and Safeguarding Policy and the relevant parts of Keeping Children Safe in Education
- Sign and follow the Staff Acceptable Use Policy and Staff Code of Conduct
- Understand that online safety is a core part of safeguarding and part of everyone's job. Record online-safety incidents in the same way as any safeguarding incident
- Know who that the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are. Notify him/her not just of concerns but also of trends and general issues you may identify.
- 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.
- 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
- 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.

11 SPIRITUAL AND MORAL VALUES LEADER (WITH RESPONSIBILITY FOR RELATIONSHIPS AND SEX EDUCATION AND PSHE)

Key responsibilities:
- As listed in the 'all staff' section, plus
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / RSE 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." Training is available at safetraining.lgfl.net
- 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.
- 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.
- Ensure that an up-to-date RSHE Policy is accessible 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

12   COMPUTING CURRICULUM 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 DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Work closely with the PSHE/RSHE Lead to avoid overlap but ensure a complementary whole-school approach
- 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

13   CURRICULUM SUBJECT 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
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Where appropriate, ensure subject specific action plans also have an online-safety element

14   NETWORK MANAGER

Key responsibilities:
- As listed in the 'all staff' section, plus:
- Collaborate with the DSL and SLT to help them make key strategic decisions around the safeguarding elements of technology.
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. 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. LGfL has a free template you can use at https://onlinesafetyaudit.lgfl.net

- Work with the DSL/OSL/DPO 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)
- 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.

15   DATA PROTECTION OFFICER (DPO)

Key responsibilities:
- Be aware of references to the relationship between data protection and safeguarding in key DfE documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools'
- 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.
- Be aware of the School's Data Retention Policy for safeguarding records
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

16   VOLUNTEERS AND CONTRACTORS (INCLUDING TUTORS)

Key responsibilities:
- Read, understand, sign and adhere to the School's Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the DSL/OSL 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
- Note that as per the school's AUP agreement, a contractor will never attempt to arrange any meeting, including tutoring sessions, 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.

17   PUPILS

Key responsibilities:

- Read, understand, sign and adhere to the Pupil AUP

18   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 and others' 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.

19   EXTERNAL USERS OF THE SCHOOL INCLUDING THE SCHOOL ASSOCIATION

Key responsibilities:

- Any external individual/organisation will sign an Acceptable Use Policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including anyone in the school community

20   EDUCATION AND CURRICULUM

The following subjects have the clearest online safety links:

- Computing
- PSHE
- Relationships and Sex Education
- 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. Whenever overseeing the use of technology, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

At Bishop Perrin School, we subscribe to Purple Mash (www.purplemash.com) to help and support our delivery of Computing and Online Safety. We also follow the online safety guidance that is laid out in the PSHE Association's

Programme of Study: www.pshe-association.org.uk/curriculum-and-resources/curriculum

Purple Mash is aligned to the National Curriculum, and within each year group's units of coverage there are dedicated lessons about online safety. These themes are covered by the following year groups:

Year 1	Logging in safely
Year 2	Creating digital footprints
Year 3	Safe passwords/fake news/age restrictions for digital media
Year 4	Awareness of identity theft/malware awareness/plagiarism/healthy screen use
Year 5	Impact of sharing information online/secure passwords/referencing sources for research/reliability
Year 6	Risks of sharing location via devices/recapping digital footprint/recapping health screen use

Regular 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.

21 HANDLING ONLINE-SAFETY CONCERNS AND INCIDENTS

It is vital that all staff recognise that online-safety is a part of our broader responsibilities of safeguarding pupils at Bishop Perrin School. Any online safety concerns must be handled in the same way as any other safeguarding concern and must be referred to the DSL.

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 any concerns to be dealt with quickly and sensitively. Any suspected online risk or infringement should be reported to the DSL/OSL as quickly as possible.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the concern is referred to the Chair of Governors and the Local Authority's Designated Officer (LADO 208 891 7370). Staff may also use the NSPCC Whistleblowing Helpline: 0800 028 0285

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The 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/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 and upskirting; see section below).

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.
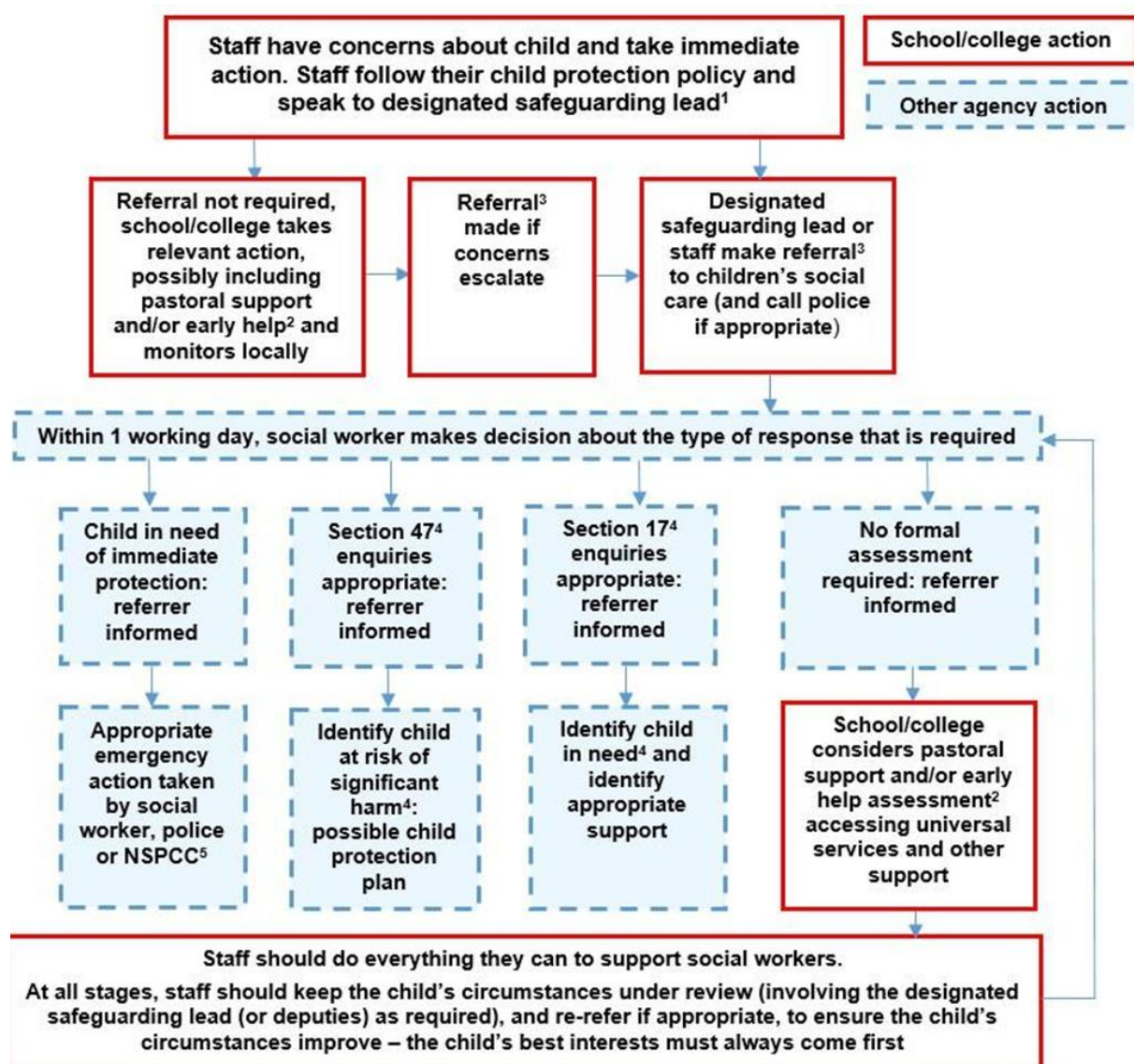
22   SEXTING-SHARING NUDES AND SEMI-NUDES

The school will follow the guidance laid out in our Child Protection and Safeguarding Policy when dealing with incidents of sexting, also referred to as 'Youth Produced Sexual Imagery' (YPSI). We will also refer to the UK Council for Internet Safety (UKCIS) guidance on sexting- 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.

In the event of an incident of YPSI occurring, staff should refer to: [Sharing nudes and semi-nudes: how to respond to an incident](#) It is a one page documents that all staff (not just classroom-based staff) can read, in recognition of the fact that it is mostly someone other than the DSL or OSL who first becomes 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 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.
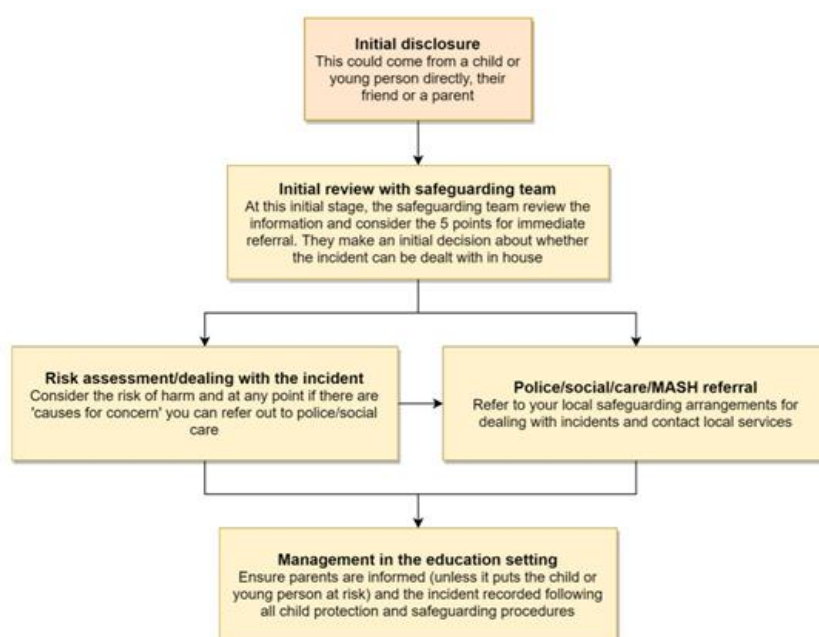
All incidents of YPSI will be dealt with as safeguarding concerns. The primary concern at all times will be the welfare and protection of the children involved. Children who share sexual imagery of themselves or their peers are breaking the law. However, as highlighted in national guidance, it is important to avoid criminalising children unnecessarily. Bishop Perrin School will therefore work in partnership with external agencies with a view to responding proportionately to the circumstances of any incident.

If the school is made aware that a nude or semi-nude image of a pupil at the school has been shared by someone else on the internet, in consultation with the parents/carers of the pupil whose image has been shared, we will support the pupil in having the image removed by using the [Report Remove tool](#) which is administered by [Childline](#).

It is important that everyone understands that whilst sexting is illegal, pupils can talk to staff if they have made a mistake or have a problem with this issue. Support for teaching about sexting can be found at [sexting.lgfl.net](#)

23   BULLYING

Online bullying will be treated like any other form of bullying and the school's Behaviour, Anti-Bullying, Exclusion and Physical Intervention Policy will be followed when dealing with an incident of online bullying (also known as cyberbullying). Staff should be aware of trends of fights being filmed and fake profiles being used to bully children in the name of others. Materials to support teaching about bullying and useful DfE guidance and case studies are at bullying.lgfl.net

24   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 can come and talk to members of staff if they have made a mistake or had a problem in this area.

25   SEXUAL VIOLENCE AND HARASSMENT

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude that "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 behaviour 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.

26   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, as well as to BYOD (bring your own device).

Where pupils contravene these rules, the school's Behaviour Policy will be applied. 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.

Increased focus on filtering and monitoring of the school's internet and systems will be shared with pupils, staff and parents via AUPs at the start of the academic year.

Where staff contravene these rules, action will be taken as outlined in the school's Capability and Disciplinary Policy.

27   SOCIAL MEDIA INCIDENTS

See the Social Media section later in this document for rules and expectations of behaviour for children and adults at Bishop Perrin School. These are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school's Behaviour, Anti-Bullying, Exclusion and Physical Intervention Policy (for pupils) and the Code of Conduct (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

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

28   DATA PROTECTION AND DATA SECURITY

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 DSLs 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**.

Bishop Perrin follows guidance about data protection from Data protection: a toolkit for schools' (April 2018)

All pupils, staff, Governors, volunteers, contractors and parents are bound by the school's Data Protection Policy and cyber security arrangements. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity

The Headteacher, DPO 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. Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The use of USO-FX and Egress to encrypt all emails that are not being sent between LGfL email accounts is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

29   APPROPRIATE FILTERING AND MONITORING

KCSiE requires schools to ensure "appropriate" webfiltering and monitoring systems which keep children safe online but do not "overblock". Since KCSIE 2023, the DSL now has lead responsibility for filtering and monitoring

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:
- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

The DSL, along with the Headteacher, Web Filtering Governor and the school's IT technicians (Click On It) will work closely to ensure the above filtering and monitoring objectives are met and regular checks are carried out.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for children to bypass systems and any potential overblocking. They can share any concerns with the DSL and may be consulted for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. Guidance and training regarding filtering, monitoring and the meaning of overblocking can be found here: https://safefiltering.lgfl.net and safetraining.lgfl.net]

At Bishop Perrin School:
- web filtering is provided by LGfL via SchoolProtect-WebScreen on school site and HomeProtect for school devices used in the home. The school also uses Senso Cloud as an additional monitoring tool: Senso.cloud | Cloud-Based Device Monitoring and Management
- changes can be made by Click On It
- overall responsibility is held by the DSL with further SLT support from the Headteacher

- technical support and advice, setup and configuration are from Click On It
- regular checks are made half termly by the DSL, in consultation with the Web Filtering Governor to ensure filtering is still active and functioning everywhere. These are evidenced in the half-termly Headteacher reports to the Full Governing Board.
- an annual review is carried out in the Autumn Term
- guidance on how the system is 'appropriate' is available at appropriate.lgfl.net

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:
- physically monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

30   ELECTRONIC COMMUNICATIONS-EMAIL

Staff at Bishop Perrin School use the LGfL StaffMail for all school emails. Pupils at this school use the LondonMail/PupilMail system from LGfL for all school emails. This is a closed email account system which only allows pupils to communicate with others within the school setting.

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

General principles for email use are as follows:

- Email is the only formal means of electronic communication to be used between staff and pupils/staff and parents (in both directions). Use of chat function on Google Classroom is allowed when in use. Use of a different platform must be approved in advance by the Headteacher/DPO. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email:
  - If data needs to be shared with external agencies, USO-FX and Egress systems are available.
  - Internally, staff should use the school network, including when working from home when remote access is available.

Pupils are able to use the Purple Mash email facility when learning about digital communications. The Purple Mash email facility only allows for internal emails to be sent, meaning that emails sent and received are for Bishop Perrin pupils only. Teachers are able to monitor emails that are sent between pupils and are also able to communicate with pupils during times of lockdown/quarantine.

- 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 school's email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored and that their emails may be read and the same rules of appropriate behaviour apply at all times. It is advisable that staff use their own personal email address for non-work related communications. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

30   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 has delegated the day-to-day responsibility of updating the content of the website to the Communications and Community Officer. The site is hosted by School Website Design Agency
https://www.schoolwebsitedesignagency.co.uk/

The Department for Education has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits to help schools to ensure that are requirements are met which can be accessed through this link: safepolicies.lgfl.net (See Appendix 4).

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. Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

31   CLOUD PLATFORMS

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

Bishop Perrin adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service.

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 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) from each organisation and stored on the school's server. Parents and staff are advised via the school's Privacy Notices.
- 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)

32   DIGITAL IMAGES AND VIDEO

When a pupil joins Bishop Perrin School, their 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). Photos and videos might be used for the following purposes:

- For displays around the school
- For the school newsletter and in reports to Governors in respect of monitoring the school's curriculum
- For the school's website
- For a specific high profile image for display, publication or broadcast (local and national media)
- For the school's Instagram account
- Marketing/publicity specifically for the school

Whenever a photo or video is taken/made, the member of staff taking it will check the parental permission slip before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name.

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 Bishop Perrin School, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos and videos are stored securely on the school network in line with the Data Retention Policy. They are reviewed annually and are deleted when no longer required. Photographs and videos of former pupils may be retained for as long as necessary for the purpose for which they were originally taken.

Parents are reminded regularly about the importance of not sharing photos and videos of children other than their own 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. Further information about this can be found in the school's Parent Acceptable Use Policy, which is linked to this guidance: parentfilming.lgfl.net

We encourage pupils to think about their online reputation and digital footprint. They 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.

33   BISHOP PERRIN'S SOCIAL MEDIA PRESENCE

Bishop Perrin 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. Negative coverage almost always causes some level of disruption.

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.

Jemma Chawla is responsible for managing our Instagram account. She follows the guidance in the LGfL/ Safer Internet Centre Online Reputation Management document here.

34   STAFF, PUPILS' AND PARENTS' SOCIAL MEDIA PRESENCE

Social media 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 AUPs 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. WhatsApp and Facebook 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's Complaints Policy should be followed. In order for a complaint to be resolved as quickly and fairly as possible, the school will ask the complainant not to discuss any details of the complaint publicly or via social media such as Facebook, WhatsApp and Twitter. Complaints will be dealt with confidentially for those involved, and we expect complainants to observe confidentiality also. Any breach of confidentiality could influence the outcome of the complaint.

Many social media platforms have a minimum age of 13 (with WhatsApp being 16+). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. 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. Parents can support their children and the school by acting as good role models as well as talking to their children about the apps, sites and games they use, with whom, for how long, and when In the Parent AUP, parents are directed to: the 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 Instagram account which is used purely to share events and activities that have occurred during school time. The school will not reply to messages sent directly to the Instagram account.

Pupils are not allowed to be 'friends' with or make a friend request to any staff, Governors, volunteers and contractors or otherwise communicate via social media. Any attempt to make requests to be 'friends' 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).

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.

Parents are discouraged from making 'friends' requests of members of staff in order for staff to maintain professional boundaries. 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, parent or staff member to the school.

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, Diocese or Richmond Council, bringing the school into disrepute.

35 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.

36 PERSONAL DEVICES INCLUDING WEARABLE TECHNOLOGY AND BRING YOUR OWN DEVICE (BYOD) POLICY

- **Pupils** in Years 5 and 6 are allowed to bring mobile phones in to school if they have permission from their parents to walk to school on their own. Mobile devices are to remain in children's lockers throughout the day and are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices. During the school day, phones must remain turned off at all times. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will be dealt with in-line with the school's Behaviour Policy and the withdrawal of mobile privileges. Pupils who are found to be using wearable technology (such as watches) to send and receive text/social media messages will have them confiscated. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All members of Bishop Perrin staff** are required to leave their mobile phones on silent during lesson time and only use them in private staff areas during break times. The exceptions to this are:
  - ✓ is if the school is operating under conditions when movement around the school and the mixing of children and adults from different classes has to be minimised. The Headteacher will inform staff when this guidance on the use of mobile phones is in place and when it is not.
  - ✓ for use in the event of Stay-inside (lockdown) procedures
- 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 put on silent. 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 or another senior member of staff should be sought and this should be done in the presence of a member staff.

- **Parents** are asked to model good mobile phone behaviour when on the school premises and to not hold lengthy private calls in the ear-shot of children and other parents when dropping off or picking up their child. Mobile phones should be put on silent and be left in bags/pockets when in the school building when attending meetings or events. Parents should ask permission before taking any photos of displays in corridors or classrooms. Any photos taken of work on display should only be of the child of the parent who is taking the photo. Photographs of work by other children are not to be taken. At no stage should photos or videos of children other than their own be taken whilst on school premises by parents unless they are captured as part of a school event such as a performance or sporting occasion. If images of children other than their own child be captured by a parent then these images are not to be shared on social media unless parents have clear consent from the parent/s of the child/ren whose images have been captured. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

37   NETWORK/INTERNET ACCESS ON SCHOOL DEVICES

- **Pupils** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use. All such use is monitored.
- **All staff who work directly with children** have access to the wireless network and networked files and drives. Full access to the networked drive is limited to senior members of staff due to confidentiality. All internet traffic is monitored.
- **Volunteers and contractors** can have access to the wireless network (on submitting a request which needs to be fully justified before being granted) but have no access to networked files/drives. All internet traffic is monitored
- **Governors** have access to the wireless network. Some Governors have limited access to networked files/drives, subject to the Acceptable Use Policy. All internet traffic is monitored.
- **Parents** can have access to the wireless network for specific events (School Association business for example) but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

38   TRIP/EVENTS AWAY FROM SCHOOL

When appropriate, staff on residential or day trips may take photos on their mobile devices which can then be sent electronically promptly back to school for distribution to parents or on the school's Instagram account. If it is not possible to send photos immediately back to the school for distribution, then they should be sent at the earliest opportunity. Any photos on staff mobiles should then be deleted immediately.

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.

39   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.

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

40   REVIEW AND MONITORING

This policy will be reviewed by the Safeguarding Governor and the Full Governing Board on a regular basis or more urgently if there is a change in legislation or recommended best practice.

APPENDICES

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
Disrespect Nobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
SWGfL	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
Parent Zone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
PSHE Association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
Educate Against Hate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	advice for schools and colleges
net-aware	NSPCC advice for parents
Common Sense Media	Independent reviews, age ratings, & other information about all types of media for children and their parents
Searching Screening and Confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGfL	Advice and resources from the London Grid for Learning

Appendix 2-Bishop Perrin Safeguarding Concern Form

Bishop Perrin Pupil Safeguarding Concern Form

Please complete this form with as much factual information (including times/dates and any direct quotes from the child) and pass it on immediately to either the Designated Safeguarding Lead (DSL) or the Deputy Designated Safeguarding Lead (DDSL).
REMEMBER-do not discuss the disclosure with anyone else except the DSL or DDSL

Child's Details			
Name:		**Class:**	

Details of Initial Cause for Concern			
Reported by:		Job Title:	
Date and time of incident:			

Your account of the concern (what was said, observed, reported and by whom):

Signed: _____   Time: _____   Date: _____

Action taken by the DSL/DDSL:

Signed: _____   Time: _____   Date: _____

Appendix 3-Sexting: How to Respond to an Incident

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.

All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.

The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People, and should not refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as **the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'. 'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention

Report it to your Designated Safeguarding Lead (DSL) immediately.

- **Never** view, download or share the imagery yourself**,** or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- **Do not** share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies should outline codes of practice to be followed.

For further information
Download the full guidance Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016) at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis.

Appendix 4-School Website RAG Audit

The school uses the LGfL School Website RAG Audit tool to assess whether the school website is compliant with expectations and legislation as laid out by the DfE.

The audit tool can be accessed via this link:

https://national.lgfl.net/digisafe/onlinesafetyaudit