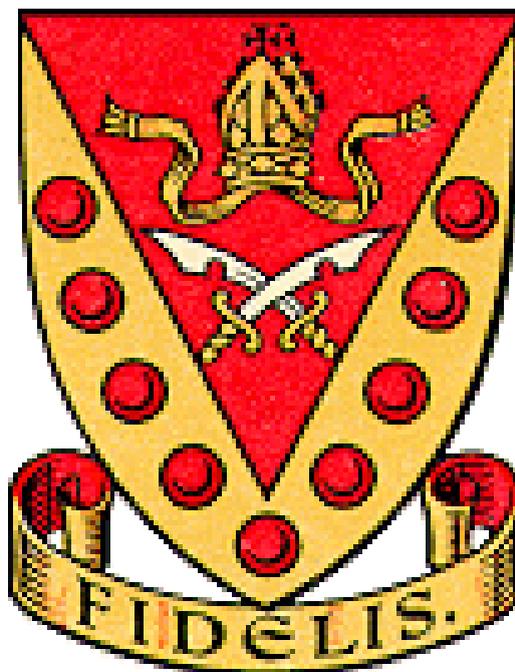# Bishopshalt School Online Safety Policy

Online Safety Policy

This Policy has been approved and adopted by Bishopshalt School in September 2021

Responsibility	Mrs R Briggs	Date reviewed	September 2021
Headteacher	Mr McGillicuddy	Next review date	September 2023
Ratified by	Governing Body	Date Ratified	September 2021

N.B. This policy is a supplemental policy to the Child Protection and Safeguarding Policy.

Contents

1. Key Contacts

Designated Safeguarding Lead (DSL)	Nigel Cockcroft	ncockroft@bishopshalt.school
Deputy Designated Safeguarding Lead	Rachel Briggs	rbriggs@bishopshalt.school
Online Safety Coordinator	Rachel Briggs	rbriggs@bishopshalt.school
IT Network Manager	Goran Milojevic Winston Durosaro	gmilojevic@bishopshalt.school wdurosaro@bishopshalt.school
Chair of Governing Board	Peter Coombs	pcoombs@bishopshalt.school
Nominated Child Protection Trustee	Gail Bond	gbond@bishopshalt.school

2. Mission and Principles

At Bishopshalt School, we encourage all our children to be active learners, to develop ideas and work to the very best of their abilities. We work with home to build and nurture their confidence, self-esteem, creativity and skills within an inclusive and caring environment.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Bishopshalt School endeavours to highlight the benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

The purpose of Bishopshalt School's online safety policy is to:

- Safeguard and promote the welfare of all members of the Bishopshalt School community online
- Identify approaches to educate and raise awareness of online safety throughout our community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to follow when responding to online safety concerns.

Bishopshalt's Safeguarding Statement
Safeguarding is everyone's responsibility

- *This school is committed to safeguarding and promoting the welfare of all children and expects all staff and volunteers to share this commitment.*

- *We seek to provide a safe and happy environment for all children*

- *This means that we have a Child Protection and Safeguarding Policy and procedures in place.*

- *All staff (including supply staff, volunteers and governors) must ensure that they are aware of these procedures.*

- *Parents and carers are welcome to read the Policy. This policy is also located on the website.*

- *Sometimes we may need to share information and work in partnership with other agencies when there are concerns about a child's welfare. We will ensure that our concerns about our pupils are discussed with his/her parents/carers first unless we have reason to believe that such a move would be contrary to the child's welfare.*

School and Local Context and Vision

Bishopshalt School is committed to safeguarding and promoting the welfare of all children and expects all staff and volunteers to share this commitment. This policy is designed to ensure all students are able to access and engage in our core values in a safe environment that removes barriers to learning. Bishopshalt identifies that the use of online platforms is increasing. Therefore, a robust online policy is to ensure students, staff, parents and the local community are best equipped with the ever changing online facilities provided to us.

Bishopshalt School works closely with the Local Authority In Hillingdon subscribing to the local vision:

The vision of the Safeguarding Children Partnership is for every child and young person to be and feel safe, enjoy good physical, emotional and mental health, have pride in their unique identities, feel they belong and have opportunities to thrive. This will involve listening to the experiences, views and aspirations of children, young people and families and ensuring that these are embedded into the Safeguarding Children Partnership's priorities and influence service provision.

All staff at Bishopshalt school are committed to actively promote the welfare of children and protect them from harm. Child protection is part of the safeguarding process. It focuses on protecting individual children identified as suffering or likely to suffer significant harm. This includes child protection procedures which detail how to respond to concerns about a child.

Through the 5 core values of the school we aim to create an environment where students can reach their full potential in a safe and caring setting, feeling secure and confident to raise any areas of concern they may have.

	Love Learning	To develop in students a love of learning. Bishopshalt students will thirst for knowledge due to the intrinsic joy that it brings.
	Show Kindness	To develop and instil in our students the virtue of kindness. Our students do things for others for no personal gain.
	Build Character	To develop in students the determination and dedication to succeed. Bishopshalt students are able to overcome any challenge that may come their way. Our students are focused, resilient and readily overcome adversity.
	Chase Brilliance	To develop students who do not settle for 'it's good enough'. Bishopshalt students always aim to improve their work and aim for perfection due to their belief that they are entitled to be brilliant.
	Bright Futures	To ensure that, for whatever field they choose to enter, Bishopshalt students succeed. Bishopshalt students will be the very best versions of themselves and compete on the world stage.

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021,'Working Together to Safeguard Children' 2018, 'Teaching Online Safety in Schools' 2019 and the local Surrey Safeguarding Children Partnership Procedures (2019)

This document should be read in conjunction with other relevant policies including, but not limited to, the School Child Protection and Safeguarding Policy, Behaviour Policy, Relationship and Sex Education Policy, Acceptable Use of Technology Policy, Staff Code of Conduct and Whistleblowing Policy.

Bishopshalt School identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material;
- **Contact:** being subjected to harmful online interaction with other users;
- **Conduct:** personal online behavior that increases the likelihood of, or causes, harm.

3. Scope

Bishopshalt School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Bishopshalt School acknowledges that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.

Bishopshalt School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners and parents and carers.

This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

All members of the school community are made aware of our expectations regarding safe and appropriate behaviour online. This is clearly outlined in our Acceptable use of Technology policies which all members of the school community are expected to sign up to.

4. Monitoring and Review

Technology evolves and changes rapidly; as such Bishopshalt School will review this policy at least annually. The policy will be revised following any national or local policy updates or developments.

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the governing body.

5. Roles and Responsibilities

The Designated Safeguarding Lead (DSL), Nigel Cockroft, and Deputy Designated Safeguarding Lead, Rachel Briggs, are recognised as holding overall lead responsibility for online safety.

Bishopshalt School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Senior Leadership Team will:

Create a culture that incorporates online safety throughout all elements of school life.

Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer/child on child abuse, use of social media and mobile technology.

Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.

Support the DSL by ensuring they have enough time and resources to carry out their responsibilities.

Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.

Undertake appropriate risk assessments, as required, regarding the safe use of technology on site.

Audit and evaluate online safety practice to identify strengths and areas for improvement.

Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.

Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

The Designated Safeguarding Lead (DSL) will:

Act as a named point of contact within the setting on all online safeguarding issues.
Liaise with other members of staff, such as Deputy DSL's, the IT technician, teaching and support staff on matters of online safety.

Ensure appropriate referrals are made to relevant external partner agencies, as appropriate. Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.

Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners safe online.

Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.

Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.

Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.

Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

Monitor online safety incidents to identify gaps and trends and use this data to update school policies and procedures.

Report online safety concerns, as appropriate, to the Leadership team. Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

Meet regularly with the governor with lead responsibility for safeguarding.

Staff will:

Contribute to the development of our Online Safety Policies.

Read and adhere to our Online Safety Policy and Acceptable Use of Technology Policies.

Take responsibility for the security of IT systems and the electronic data they use or have access to.

Model good practice when using technology with learners

Maintain a professional level of conduct in their personal use of technology, both on and off site.

Embed online safety education in curriculum delivery wherever possible.

Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.

Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.

Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.

Take personal responsibility for professional development in this area.

Staff managing the technical environment will:

Provide technical support and perspective to the DSL and school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

Implement appropriate security measures as directed by the leadership team to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

Learners (at a level that is appropriate to their individual age and ability) will:

Engage in age/ability appropriate online safety education.

Contribute to the development of online safety policies.

Read and adhere to the Acceptable Use of Technology and Behaviour Policies.

Respect the feelings and rights of others, on and offline.

Take an appropriate level of responsibility for keeping themselves and others safe online.

Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

Parents and Carers will:

Read our Acceptable Use of Technology Policies and encourage their children to adhere to them.

Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

Role model safe and appropriate use of technology and social media.

Seek help and support from school or other appropriate agencies, if they or their child encounter online issues.

Contribute to the development of our online safety policies.

Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies their children access and use at home.

6. Education and engagement with learners

The school will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:

- ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework - 2020' and DfE 'Teaching online safety in school' guidance;
- ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education and Computing programmes of study;
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site;
- implement appropriate peer education approaches through our Tutor Time Programme
- creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online;
- involving the DSL (or DDSL) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content;
- making informed decisions to ensure that any educational resources used are appropriate for our learners;
- using external visitors, where appropriate, to complement and support our internal online safety education approaches;
- providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.

Bishopshalt School school will support learners to understand and follow our Acceptable Use of Technology Policies in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access.
- informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

Bishopshalt School school will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age appropriate education regarding safe and responsible use precedes internet access;

- teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable;
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation;
- enabling them to understand what acceptable and unacceptable online behaviour looks like;
- preparing them to identify possible online risks and make informed decisions about how to act and respond;
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Learners

Bishopshalt School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may require additional support in staying safe online.

Bishopshalt School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
Staff will seek input from specialist staff as appropriate, including the DSL, Deputy DSLs, SENDco and IT Manager to ensure that the policy and curriculum is appropriate for all learners.

7. Training and engagement with staff

We will:

Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

Provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be part of our annual safeguarding and child protection training for all staff.

Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations;

Build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.

Make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

Make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.

Highlight useful educational resources and tools which staff could use with learners.

Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

8. Awareness and engagement with parents and carers

Bishopshalt School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- providing information and guidance on online safety in a variety of formats. This will include highlighting on-line safety events such as parent evenings and transition events;
- drawing their attention to our online safety policy and expectations in our newsletters and other external communication;
- requesting parents and carers read online safety information when joining our community.

9. Reducing Online Risks

Bishopshalt School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our Acceptable Use of Technology Policies and highlighted through a variety of education and training approaches.

10. Safer Use of Technology

Classroom use

Bishopshalt School uses a wide range of technology. This includes access to;

- Computers, laptops, tablets, mobile phones and other digital devices
- Internet, which may include search engines and educational websites
- Learning platform/intranet
- Email
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our Acceptable Use of Technology Policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use appropriate search tools as identified following an informed risk assessment:

- Google and Bing "SafeSearch" enforced by filtering policy;
- Suspicious search queries report generated weekly and emailed to the IT Manager and DSL for review;
- The use of AB Tutor software and LGFL blocking systems
- Staff to report inappropriate search results to the IT Manager and DSL.

We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledges the source of information.

Supervision of internet access and technology use will be appropriate to learners age and ability.

Key Stage 3 and 4

Learners will use age-appropriate search engines and online tools.

Learners will be appropriately supervised during lessons when using technology, according to their ability and understanding.

Learners may have access to technology unsupervised, however appropriate levels of filtering and monitoring will be in place.

Key Stage 5

Learners will use age appropriate search engines and online tools.

Learners will be able to use technology unsupervised, however appropriate levels of filtering and monitoring will be in place.

11. Managing internet access

We will maintain an online record of users who are granted access to our devices and systems.

All staff, learners and visitors will read and agree an Acceptable Use Policy before being given access to our computer system, IT resources or the internet.

12. Filtering and monitoring

Leaders, managers and DSLs can access the guidance for education settings about establishing 'appropriate levels' of filtering and monitoring to help inform their decision making:
www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Decision making

Bishopshalt School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Appropriate filtering

Bishopshalt School's education broadband connectivity is provided through London Grid For Learning (LGFL).

Bishopshalt School uses LGFL filtering system

LGFL blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

LGFL is a member of [Internet Watch Foundation](#) (IWF) and blocks access to illegal Child Abuse Images and Content.

LGFL integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

We work with LGFL and AB Tutor to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

If learners or staff discover unsuitable sites or material, they are required to turn off monitor/screen, report the concern immediately to a member of staff, report the URL of the site to technical staff/services.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving learners.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

We will appropriately monitor internet use on all settings owned or provided internet enabled devices. This is achieved by:
- Physical monitoring
- Review of AB tutor
- Logs/reports
- Safeguarding software (LGFL and AB Tutor)

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

If a concern is identified via monitoring processes the IT Network Manager and DSL will respond in line with the child protection and safeguarding policy.

13. Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Full information can be found in the [Bishopshalt Data Protection GDPR Policy](#)

14. Security and management of information systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly;
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems;
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use;
- Not downloading unapproved software to work devices or opening unfamiliar email attachments;
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools;
- Checking files held on our network, as required and when deemed necessary by leadership staff;
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all users;
- All users are expected to log off or lock their screens/devices if systems are unattended.

15. Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- All learners have their own unique username and private passwords to access our systems, learners are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system;
    - change their passwords as instructed;
    - not share passwords or login information with others or leave passwords/login details where others can find them;
    - not to login as another user at any time;
    - lock access to devices/systems when not in use.

16. Managing the safety of our website

We will ensure that information posted on our website meets the requirements as identified by the DfE.

We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

17. Publishing images and videos online

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the Photography and Filming Policy, Data Security, Acceptable Use of Technology Policy and Codes of Conduct.

18. Managing email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, Acceptable Use of Technology Policies and the Code of Conduct.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

Setting email addresses and other official contact details will not be used to set up personal social media accounts.

Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff email

All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents. Staff are encouraged to copy in their line manager when replying to parent emails that are subject related. Pastoral emails must include the relevant head of year. Where a safeguarding concern is raised via email, this should be reported to DSL and Deputy DSL by forwarding the email as a matter of priority.

Communication with parents is logged centrally on CPOMS. It is important that if not copied in, staff summarise and inform the head of year of any issues that have arisen. Support for staff can then be put in place where needed.

During school holidays, staff should switch their email to 'out of hours'. Any necessary communication can be done through the school office email. DSL, Deputy DSL and Miss Colley will continue to access safeguarding emails.

Learner email

Learners will use a provided email account for educational purposes.

Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email use before access is permitted.

Whole-class or group email addresses will be used for communication outside of the setting other than when providing feedback on work completed.

19. Educational use of videoconferencing and/or webcams

Logi cameras are set up on classroom computers due to the increasing use for online lessons.
Staff have a responsibility to ensure these are used appropriately and for school lessons, school business meetings and parent consultations via School Cloud only.

20. Management of learning platforms

Bishopshalt School uses google as an official learning platform.

Leaders and staff will regularly monitor the usage of the Learning Platform, including message/communication tools and publishing facilities.

Only current members of staff, learners and parents will have access to the Learning Platform. When staff and/or learners leave the setting, their account will be disabled.

Parents and staff will be advised about acceptable conduct and use when using the Learning Platform.

All users will be mindful of copyright and will only upload appropriate content onto the Learning Platform.

Any concerns about content on the Learning Platform will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive;
- If the user does not comply, the material will be removed by the site administrator;

- Access to the Learning Platform for the user may be suspended;
- The user will need to discuss the issues with a member of leadership before reinstatement;
- If the content is illegal, we will respond in line with existing child protection procedures.

A visitor may be invited onto the Learning Platform by a member of the leadership team as part of an agreed focus or a limited time slot.

21. Management of applications (apps) used to record children's progress

We use Bromcom to track learners progress and share appropriate information with parents and carers.

The Headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data
- only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs;
- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images;
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft;
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems;
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

22. Use of Social Media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the school community.

The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.

All members of the school community are expected to engage in social media in a positive and responsible manner.

All members of the school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control learner and staff access to social media whilst using school provided devices and systems on site.

- The use of social media during school hours for personal use is not permitted for staff
- The use of social media during school hours for personal use is not permitted for learners
- The use of Social media sites is restricted to the Headteacher and Business manager by filtering policy
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.

Concerns regarding the online conduct of any member of the school community on social media, will be reported to the DSL and be managed in accordance with our child protection and safeguarding policy and code of conducts.

Staff personal use of social media

The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our staff code of conduct and acceptable use policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school

Disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:

- Setting appropriate privacy levels on their personal accounts/sites;
- Being aware of the implications of using location sharing services;
- Opting out of public listings on social networking sites;
- Logging out of accounts after use;
- Using strong passwords;
- Ensuring staff do not represent their personal views as being that of the school.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use

is compatible with their professional role and is in accordance with our policies, and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.

All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the Headteacher.

Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.

If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

Any communication from learners and parents received on personal social media accounts will be reported to the DSL and the Headteacher.

Learners use of social media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.

We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including the behaviour policy.

Concerns regarding learners' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Learners will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location;
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private;
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present;
- to use safe passwords;
- to use social media sites which are appropriate for their age and abilities;
- how to block and report unwanted communications;
- how to report concerns on social media, both within the setting and externally.

Official use of social media

Bishopshalt School's official social media channel is:

- Twitter

The official use of social media sites by Bishopshalt School only takes place with clear educational or community engagement objectives and with specific intended outcomes.

- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

- Staff use setting provided email addresses to register for and manage official social media channels.
- Official social media sites are suitably protected and, where possible, run and are linked to our website.
- Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including but not limited to behaviour, photography and filming, data protection, child protection and safeguarding.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving learners will be moderated if possible.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
- Be aware they are an ambassador for the setting.
- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

23. Mobile Technology: Use of Personal Devices and Mobile Phones

Bishopshalt School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Expectations

All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as the behaviour policy and child protection and safeguarding policy and with the law.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- All members of Bishopshalt School community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

- All members of Bishopshalt School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms and toilets.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our behaviour policy and code of conducts.

All members of Bishopshalt School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection and safeguarding policies.

Staff use of personal devices and mobile phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection and safeguarding, data security and acceptable use.

Staff will be advised to
- keep mobile phones and personal devices in a safe and secure place e.g. locked in a locker/drawer or cupboard during lesson time.
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- not use personal devices during teaching periods, unless written permission has been given by the Headteacher such as in emergency circumstances.
- ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are only permitted to use their own personal phones or devices for contacting learners or parents and carers in exceptional circumstances with the permission of the Headteacher.
- Any pre-existing relationships which could undermine this, will be discussed with the DSL and Headteacher.

Staff will not use personal devices or mobile phones:
- to take photos or videos of learners and will only use work-provided equipment for this purpose.
- directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our staff code of conduct and child protection and safeguarding policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our child protection and safeguarding policy.

Learners use of personal devices and mobile phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

- Bishopshalt School expects learners' personal devices and mobile phones to be kept in a secure place during the school day.

If a learner needs to contact his/her parents or carers they will be allowed to use the pupils office school phone.

- Parents are advised to contact their child via the school office, exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.

Mobile phones or personal devices will not be routinely used by learners during lessons or formal educational time.

- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene the child protection and safeguarding or behaviour policy.
- Searches of mobile phone or personal devices will be carried out in accordance with *Searching, Screening and Confiscation'*
- Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. In line with the DfE *'Searching, Screening and Confiscation'*
- Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the school day or week.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' use of personal devices and mobile phones

Parents/carers and visitors, including volunteers and contractors will be informed that mobile phones are only permitted within specific areas of the school.

Information is provided at signing in to inform parents/carers and visitors of expectations of use.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance

with our acceptable use policy and other associated policies, including but not limited to behaviour, child protection and safeguarding and filming and photography.

Members of staff are expected to challenge visitors if they have concerns and inform the DSL or Headteacher of any breaches of our policy.

Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

School mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

24. Responding to Online Safety Incidents

All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer/child on child abuse, including cyberbullying and youth produced sexual imagery (sharing of nudes and semi - nudes), online sexual violence and harassment, online abuse and exploitation and illegal content.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
   - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Service.

Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the Headteacher will speak with the police and the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

Concerns about learner online behaviour and/or welfare

The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.

All concerns about learners will be recorded in line with our child protection and safeguarding policy.

Bishopshalt School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer/child on child abuse concerns will be responded to in line with our child protection and safeguarding and behaviour policies.

The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate.

We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Concerns about staff online behaviour and/or welfare

Any complaint about staff misuse will be referred to the Headteacher in accordance with our child protection and safeguarding policy and code of conduct.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appropriate action will be taken in accordance with our staff code of conduct.

Welfare support will be offered to staff as appropriate.

Concerns about parent/carer online behaviour and/or welfare

Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher. The headteacher will respond to concerns in line with existing policies, including but not limited to child protection and safeguarding, complaints, staff code of conduct, acceptable use and behaviour policy.

Appropriate action will be taken, if necessary, in line with child protection and safeguarding policy and the staff code of conduct.

Welfare support will be offered to parents/carers as appropriate.

25. Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children
www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

Our headteacher, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2020.

- Full details of our response to peer on peer/child on child abuse, including sexual violence and harassment can be found in our child protection and safeguarding policy.

Bishopshalt School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;

- Non-consensual sharing of sexual images and videos
- Sexualised online bullying
- Online coercion and threats
- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL and act in accordance with our child protection and safeguarding and behavior policies.
- if content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy.
- inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make referrals to partner agencies, such as Children's Services and/or the police.

- if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

26. Youth produced sexual imagery ("sexting")

Bishopshalt School recognises youth produced sexual imagery (also known as "sharing of nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

We will follow the advice as set out in the non-statutory UKCIS guidance: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#).
- Youth produced sexual imagery or 'sharing of nudes and semi nudes' 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 an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:
- view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
- If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
- send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
- act in accordance with our child protection policies and the relevant local procedures.
- ensure the DSL responds in line with the UKCIS and SSCP guidance.
- Store any devices containing potential youth produced sexual imagery securely
- If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- carry out a risk and needs assessment in line with the UKCIS and SSCP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- make a referral to Children's Services and/or the police, as deemed appropriate in line with the UKCIS and SSCP guidance.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

27. Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

Bishopshalt School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection and safeguarding policy.

We will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community.

If made aware of an incident involving online child abuse and/or exploitation, we will:
- act in accordance with our child protection and safeguarding policy and the relevant SSCP procedures.
- store any devices containing evidence securely.
  - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
- if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Service and/or police.

If made aware of intelligence or information which may relate to child exploitation (on or offline), it will be passed through to the police by the DSL.

If members of the public or learners at other settings are believed to have been targeted, the DSL will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

28. Indecent Images of Children

Bishopshalt School will ensure that all members of the community are made aware of the possible consequences of accessing indecent images of children as appropriate to their age and ability.

We will respond to concerns regarding indecent images of children on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to indecent images of children by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Education Safeguarding Service.

If made aware of indecent images of children, we will:
- act in accordance with our child protection policy and the relevant SSCP procedures.
- store any devices involved securely.
- immediately inform appropriate organisations, such as the IWF and police.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- ensure that any copies that exist of the image, for example in emails, are deleted.
- report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:
- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Services, as appropriate.
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
- report concerns, as appropriate to parents/carers.

If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
- ensure that the Headteacher is informed in line with our child protection and safeguarding policy.

- inform the LADO and other relevant organisations in accordance with our child protection and safeguarding policy.
- quarantine any devices until police advice has been sought.

29. Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Bishopshalt School and full details of how we will respond to cyberbullying are set out in Bishopshalt Anti Bullying Policy

30. Online hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated and will be responded to in line with existing policies, including child protection and safeguarding, anti-bullying and behaviour policies.
All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Service and/or the police.

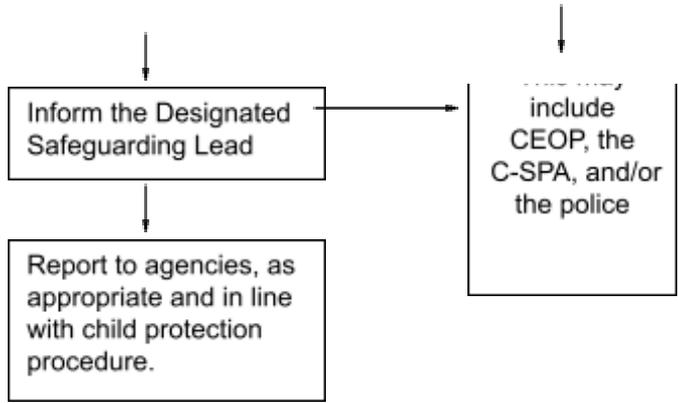## 31. Online radicalisation and extremism

As referenced in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection and safeguarding policy.
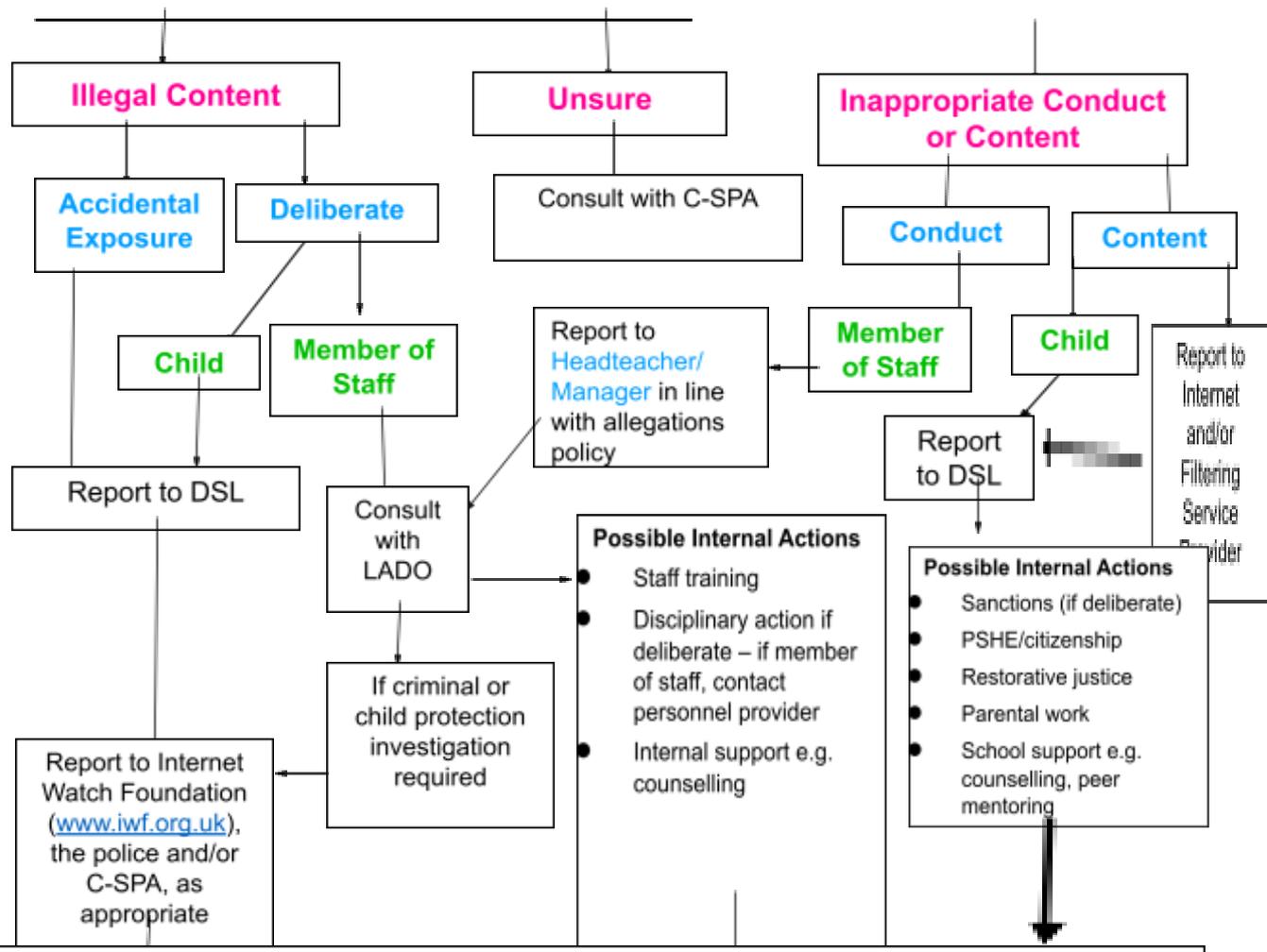
If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and safeguarding policy.

Responding to an Online Safety Concern Flowchart

Conduct   Online Safety Concern

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, the C-SPA, and/or the police

Key Contacts
Designated Safeguarding Lead: Nigel Cockroft

Deputy Designated Safeguarding Lead: Rachel Briggs

Headteacher: Liam McGillicuddy

School Office: 01895 233909

Police: 101 or 999 if immediate risk of harm

Illegal Content

Accidental Exposure   **Deliberate**

Child   **Member of Staff**

Report to DSL

Consult with LADO

If criminal or child protection investigation required

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or C-SPA, as appropriate

Unsure

Consult with C-SPA

Report to Headteacher/ Manager in line with allegations policy

Possible Internal Actions
- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling

Inappropriate Conduct or Content

Conduct   **Content**

Member of Staff   **Child**

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions
- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Parental work
- School support e.g. counselling, peer mentoring

Record incident, action taken and decision making in line with child protection recording systems. Review policies and procedures and implement changes

33.Useful Links

Hillingdon Children's Safeguarding Website: [Hillingdon Children's Safeguarding](#)
01895 556006

**Stronger Families Hub: referral making**
[Stronger Families](#)

Surrey Police:
[Hillingdon Police](#)
In an emergency (a life is in danger or a crime in progress) dial 999.

For non-urgent enquiries, contact Hillingdon Police via 101

National Links and Resources for Schools, Learners and Parents/Carers

Reporting Harmful Content

 https://www.iwf.org.uk/

 https://reportharmfulcontent.com/

 https://ceop.police.uk/safety-centre/
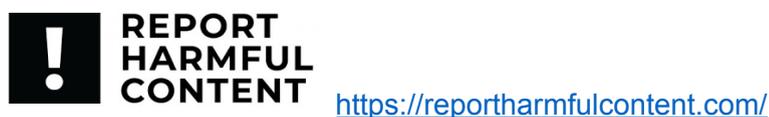
Websites to visit for online safety information:

 Think U know: www.thinkuknow.co.uk

Thinkuknow is the education programme from The National Crimes Agency's Child Exploitation and online Protection Centre (CEOP). The website is suitable for children aged 5-16 and has a section for parents/carers.

Net Aware NSPCC: www.net-aware.org.uk and www.nspcc.org.uk/onlinesafety

Resources produced by the NSPCC for parents, including Net Aware, a tool which reviews the most popular apps. They also provide advice on 'sharing of nudes and semi nudes', online gaming and parental controls. The NSPCC helpline number is 0808 8005002

ChildLine: www.childline.org.uk

The ChildLine website provides information and advice on a wide range of issues including online and offline safety. Advice includes using social media, cyberbullying, online grooming, taking care of your digital footprint and mobile phone safety. The ChildLine helpline is 0800 1111

Zipit App: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/zipit-app/

Zipit is an app designed in conjunction with Childline to help young people decline requests for nudes and inappropriate content.

https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/

Another app supported by Childline to assist young people in removing nudes from the internet.

UK Safer Internet Centre: www.saferinternet.org.uk

UK Safer Internet Centre provides online safety tips, advice and resources to help children and young people stay safe online. Advice also includes setting up parental controls and what to consider before buying mobile devices.

Childnet: www.childnet.com

Childnet has resources, including videos and storybooks, to help you discuss online safety with your children. It includes advice on setting up parental controls, cyberbullying and setting up a family agreement for safer internet use. It has a parent and carer toolkit. Childnet have produced smart rules for online safety, using Widget symbols; these can be displayed near computers as a visual reminder. They have also produced the STAR SEN Toolkit to explore online safety with young people who have special educational needs.

Internet Matters: www.internetmatters.org

Internet Matters provides advice by age group. Advice incudes setting up appropriate controls and filters on a range of devices, cyberbullying, online grooming and self-harm.

Parent Info: www.parentinfo.org

Parent Info provides information to parents and carers about a wide range of topics including games, apps and tech, health and wellbeing.

BBC "Own It" Website and App: www.bbc.com/ownit and ww.bbc.com/ownit/take-control/own-it-app

The BBC Own It Website provide advice for parents and carers and aims to help children aged 8-13 "be the boss" of their online lives. The website has videos and activities to explore with children and includes an app which can be downloaded (for children aged 8+) on children's devices to help them use technology safely and responsibly.