Bushbury Hill Primary School

'To be the best that we can be'

Online Safety & Acceptable Use Policy

Document Holder	Charlie Price
Date Approved By Governors	December 2024
Review Date	November 2026

Bushbury Hill Primary School’s Online Safety Policy

Designated Safeguarding Lead:	**Charlotte Underwood**
Online Safety Lead:	**Charlie Price**
Named Governor with lead responsibility:	**Victoria Chalmers (currently on maternity)** **Alan Jasper**

1. Policy aims

- This online safety policy has been written by Bushbury Hill Primary School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance ‘Keeping Children Safe in Education’ 2022, Early Years and Foundation Stage 2017 ‘Working Together to Safeguard Children’.
- This policy should also be read in conjunction with Ofsted’s ‘Review of sexual abuse in schools and colleges’ and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people and DfE Behaviour in Schools 2022.

- The purpose of Bushbury Hill Primary School online safety policy is to
  - safeguard and promote the welfare of all members of Bushbury Hill Primary 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.

- Bushbury Hill Primary School identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk, as identified in KCSIE 2022.
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
  - **Commercial:** risks such as: online gambling, access to inappropriate advertising, phishing, in-game purchasing and or financial scams

2. Policy scope

- Bushbury Hill Primary 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.
- Bushbury Hill Primary School identifies 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.

- Bushbury Hill Primary 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, learning support assistants, learning mentors, lunchtime learning and play leaders, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (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.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
    - Behaviour and discipline policy
    - Child protection policy & Safeguarding
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security
    - Cameras and image use policy
    - Mobile phone and social media policies
    - Searching, screening and confiscation *policy*
    - Harmful sexual Behaviour policy

3. Monitoring and review

- Technology evolves and changes rapidly; as such Bushbury Hill Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- 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/online safety lead 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 wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Charlotte Underwood - Headteacher) is recognised as holding overall lead responsibility for online safety, in line with KCSIE 2022.
- Bushbury Hill Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 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 the online safety lead, pastoral support staff, IT technicians, network managers and the SENCO 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 the online safety lead to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- 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 the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the online safety Lead, school management team and Governing Body.
- Work with the online safety lead to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet half termly with the online safety Lead to report on online safety issues and develop and action plan for the following term.

4.2 The online safety Lead will:

- Create a whole setting 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 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.
- Meet termly with the governor with a lead responsibility for safeguarding and online safety.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Support the DSL and any deputies 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 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.
- Support the Year 6 group of Digital Ambassadors to promote the importance of online safety in school.
- Lead termly online safety sessions to ensure that online safety is promoted to parents, carers and the wider community.
- Liaise with outside agencies e.g. CEDOB. 7
- Develop a planned and coordinated online safety education programme. This will be provided through:
    - a discrete Online Safety long term plan – Project Evolve
    - PHSE and SRE programmes (work with Thematic Curriculum Lead-KAPOW)
    - assemblies and pastoral programmes
    - through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

4.3 It is the responsibility of all members of staff to:

- 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's 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.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL, Online Safety Lead and school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including as directed by the leadership team to ensure that the settings 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 headteacher and online safety lead.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL to enable them to take appropriate safeguarding action when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- 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.

4.6 It is the responsibility of parents and carers to:

- 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 and abide by the parental acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.

- Use our systems, such as Facebook, Class Dojo and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting 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' and DfE 'Teaching online safety in school' guidance.
    - Delivering an online safety curriculum using Project Evolve, supported by our RSHE curriculum (KAPOW).
    - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship 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.
    - implementing appropriate peer education approaches using the Digital Ambassador programme (training of which is provided by staff from Wider Learning and work continued with the group by the Online Safety Lead).
    - 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 and Online Safety Lead 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, (e.g. The Centre for Digital and Online Behaviours) 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.
    - rewarding positive use of technology (TT Rockstars, Spelling Shed weekly certificates for online achievements using safe online resources outside of the classroom)
- Bushbury Hill Primary School will support learners to understand and follow our acceptable use 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.
- Bushbury Hill Primary 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.

5.2 Vulnerable Learners

- Bushbury Hill Primary 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 have less support in staying safe online.
- Bushbury Hill Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at Bushbury Hill Primary School will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 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. Training will be provided through annual safeguarding and child protection training, an annual online safety staff meeting and through updates when needed from the DSL or Online Safety Lead.
    - ensure 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 provide 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.

5.4 Awareness and engagement with parents and carers

- Bushbury Hill Primary 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 be addressed via termly parent Online Safety sessions, Safe Website guides, Posts on the schools social media systems (Class Dojo and Facebook) and the option to request meetings/support when needed from the Online Safety Lead.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters, Facebook and Class Dojo) as well as in our prospectus and on our website.
  - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Bushbury Hill Primary 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 in the school 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.

7. Safer Use of Technology

7.1 Classroom use

- Bushbury Hill Primary School uses a wide range of technology. This includes access to
  - Computers, laptops, tablets and other digital devices
  - Internet, which may include search engines and educational websites
  - Class Dojo/Learning platform
  - Email (KS2 Only)
  - 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.
  - The measures in place for tablets are: regular password changes, devices will be wiped termly and tracking will be set up on all devices.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. Staff will be advised to use Safeyoutube.net to enable safe use of videos from YouTube (removal of adverts/additional content/comments).
- The setting will use appropriate search tools as identified following an informed risk assessment.
  - EYFS/KS1 will use SWGfL Swiggle and KS2 will use Google as their specific search engines.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learner's age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learner's age and ability eg via Air Drop on iPads
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learner's age and ability eg via Microsoft Teams

7.2 Managing internet access

- We will maintain a written 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.

7.3 Filtering and monitoring

7.3.1 Decision making

- Bushbury Hill Primary School's 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.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- 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.

7.3.2 Appropriate filtering

- Bushbury Hill Primary's education broadband connectivity is provided through City of Wolverhampton Council who use Virgin Media.
- Bushbury Hill Primary's uses Lightspeed
  - Lightspeed 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.
  - Lightspeed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
  - Lightspeed integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with Wolverhampton eServices and City of Wolverhampton Council 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 online safety lead who will inform technical staff/services.

- Filtering breaches will be reported to the online safety lead who will inform DSL (or deputy) and technical staff – this will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners where appropriate (this decision will be made by the online safety lead in collaboration with the DSL).
- 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.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - *physical monitoring (supervision),*
    - *monitoring internet and web access (reviewing log file information from Lightspeed when requested).*
    - *active/pro-active technology monitoring services (Senso).*
- 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 approaches it will be dealt with by *DSL or deputy will respond in line with the child protection policy and staff handbook/AUPs.*

7.4 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 our information security policy which can be accessed by request.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- devices will be password protected. (Be sure to select devices that can be protected in this way)
- devices will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they: (schools may wish to include more detail about their own data/password/encryption/secure transfer processes)

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. encrypted cloud systems)

- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

7.5 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 – this includes not turning off proxy settings whilst in school.
    - 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.

7.5.1 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.
- From years 2-6, all learners are provided with 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 – staff must change the default laptop password to a strong password following best practise guidelines.
    - change their passwords regularly (staff are prompted to change their Office 365 passwords regularly).
    - change their password if they feel it has been compromised.
    - 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.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE. Our website is managed by Wolverhampton eServices who are responsible for ensuring our compliance.
- 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.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

7.8 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/behaviour policy.
- 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. Staff should only use recognised school email systems in relation to work.
- 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 (Charlotte Underwood DSL/Headteacher and/or Charlie Price Online Safety Lead) 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 will be blocked on site.

7.8.1 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, learners and parents.

- Staff emails can be accessed when not on site but it cannot be expected that these will always be checked or responded to beyond the school's working hours.

7.8.2 Learner email

- Learners in Years 5 and 6 may use a provided email account for educational purposes.
- All learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.10 Management of Online Learning Spaces (OLS)

- Bushbury Hill Primary School uses Class Dojo and Microsoft Teams as official learning spaces.
- Leaders and staff will regularly monitor the usage of these spaces, including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access – parents can only see their child/children on Class Dojo via their login and are only able to have access to Microsoft Teams when their child logs in. Parents do not have permission to post within Microsoft Teams.
- When staff *and/or* learners leave the setting, their account will be disabled or transferred to their new establishment/Year group.
- Learners and staff will be advised about acceptable conduct and use when using the OLS.
- All users will be mindful of copyright and will only upload appropriate content onto the OLS.
- Any concerns about content on the OLS 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 OLS for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame eg. Digital Ambassador.
- A visitor may be invited onto the OLS by a member of the leadership as part of an agreed focus or a limited time slot.

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

- We use 2build a profile and Class Dojo to track learners' progress and share appropriate information with parents and carers.
- The headteacher/online safety lead 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.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Bushbury Hill Primary 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 Bushbury Hill Primary School community are expected to engage in social media in a positive and responsible manner.
    - All members of Bushbury Hill Primary 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 as these sites are blocked using our filtering system except for the Headteacher, Deputy and Computing Lead who have permission to access the school's official Facebook account.
    - The use of social media during school hours for personal use is not permitted for staff unless it is during their personal break times out of sight of all children.
    - The use of social media during school hours for personal use is not permitted for learners.
    - Inappropriate 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 Bushbury Hill Primary School community on social media, will be reported to the DSL/Online Safety Lead and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 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 code of conduct/behaviour policy, social media policy and acceptable use of technology policy.

8.2.1 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.
  - Civil, legal or 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 setting.
- Members of staff are encouraged not to identify themselves as employees of Bushbury Hill Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- 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 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.

8.2.2 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 DSL/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, Deputy DSL or Online Safety Lead.

8.3 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 anti-bullying and behaviour.
- 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.

8.4 Official use of social media

- Bushbury Hill Primary School's official social media channels are:
    - Facebook
- The official use of social media sites by Bushbury Hill Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher, Computing Lead/Online Safety Lead.

    - The Headteacher, Deputy Headteacher and Computing Lead/Online Safety Lead 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 linked from 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 anti-bullying, image/camera use, data protection, confidentiality and child protection.
- 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.
- 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.

8.4.1 Staff expectations

- Members of staff are advised to follow but not ‘like’ the school’s official Facebook page to avoid making their personal accounts visible and 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:
    - Sign our social media acceptable use policy.
    - 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 (or deputy) and/or the Online Safety Lead of any concerns, such as criticism, inappropriate content or contact from learners.

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

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

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of Bushbury Hill Primary 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 Bushbury Hill Primary 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 where children are present unless in an emergency situation (ie.to contact school whilst up at the Canopy/Muga or on the school field).
- 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 anti-bullying and behaviour policies.
- All members of Bushbury Hill Primary 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 policies.

9.2 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, data security and acceptable use of technology.
- Staff will be advised to
    - keep mobile phones and personal devices in a safe and secure place (locked in a cupboard/drawer) 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 not permitted to use their own personal phones or devices for contacting learners or parents and carers.
  - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) 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 behaviour and allegations 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 allegations policy.

9.3 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.
  - Bushbury Hill Primary School expects learners' personal devices and mobile phones that need to be brought on site to be handed in at the office on arrival to school and collected again at the end of the school day. These devices need to be switched off prior to being handed in.
- If a learner needs to contact his/her parents or carers a member of the office team will complete this on their behalf.
  - Parents are advised to contact school to provide messages that may need to be passes on to their child.
- Mobile phones or personal devices will not be used by learners at all whilst on site.
- Mobile phones and personal devices must not be taken anywhere on site and will lead to their device being confiscated and a possible ban from being able to bring their device to school at all.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
  - Staff may confiscate a learner's mobile phone or device if they found to have it in their possession whilst in school.
  - Searches of mobile phone or personal devices will be carried out in accordance with our policy and with the DfE 'Searching, Screening and Confiscation' guidance.

    - Learners' mobile phones or devices may be searched by the Headteacher or Online Safety Lead, ideally with the consent of the learner or a parent/ carer. However, the school can search without consent as per the DfE guidance. Content may be deleted or requested to be deleted, if it contravenes our policies. This will be completed in accordance with the DfE 'Searching, Screening and Confiscation' guidance.
    - Mobile phones and devices that have been confiscated will be released to parents/ carers/children (as necessary) at the end of the school day.
    - 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.

9.4 Visitors' use of personal devices and mobile phones

- Parents/carers and visitors, including volunteers and contractors, should ensure that they will leave their phone in their pocket where possible. Under no circumstances will they use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), they will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- Parents are permitted to use personal devices to capture video and images at agreed school productions e.g. Graduation ceremonies (there may be occasions, for copyright and safeguarding reasons, where this is not the case). However, where possible the recording/image will only be of their child and where it contains other children (e.g. the background) they will be advised not to upload and share on Social Media unless they have specific permission from the parents of all children within the recording/image.

- Appropriate signage and information is provided 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 of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy), Headteacher or Online Safety Lead of any breaches of our policy.

10. 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 abuse, including cyberbullying and youth produced sexual imagery (sexting), 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 (or deputy) 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 DSL Headteacher will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) or Online Safety Lead 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 policy.
- Bushbury Hill Primary 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 abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) or Online Safety Lead 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. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy/code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher DSL (or deputy) or the Online Safety Lead. The Headteacher DSL (or deputy) or the Online Safety Lead will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- Our headteacher, DSL and appropriate members of staff have accessed and understood Ofsted's 'Review of sexual abuse in schools and colleges' (2021) recommendations and part 5 of 'Keeping Children Safe in Education' 2024
  - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our safeguarding & child protection policy and in our Harmful Sexual Behaviour policy
- We take the view that **'it could happen here'** and recognise 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 (or deputy) and act in accordance with our child protection and anti-bullying 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 Social Work Service 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 (or deputy) 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.
- Bushbury Hill Primary School recognises that 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.
- Bushbury Hill Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Bushbury Hill Primary School 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.

11.2 Youth produced sexual imagery ("sexting")

- Bushbury Hill Primary School recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
    - We will follow the advice as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes Advice for education settings working with children and young people Responding to incidents and safeguarding children and young people.
    - Youth produced sexual imagery or '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 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.
- Bushbury Hill Primary School 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. Members of the community can access support from the links on the schools website, learning platform or on the staff room noticeboard where appropriate.

- 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 (or deputy) responds in line with the UKCIS and KSCMP 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 assessment in line with the UKCIS and KSCMP 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 Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP 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.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Bushbury Hill Primary 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 (or deputy), in line with our child protection policy.

- Bushbury Hill Primary School 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. This can be accessed on the schools website and learning platform.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP 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 (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service

before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Bushbury Hill Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC 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 (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP 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 (or deputy) 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 (or deputy) 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 Social Work Service, 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 managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
    - quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Bushbury Hill Primary School
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which can be found on the school's website or as a paper copy displayed in the staffroom.

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Bushbury Hill Primary School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- 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 (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed 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 (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that 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 allegations policies.

11.8 Online safeguarding trends

Over the past year, our school has observed several concerning trends regarding device use, misuse, and online incidents that impact the wellbeing and safety of our students.

Nationally, some key trends from the past year are outlined below, which are reflected in our policy and acceptable use agreements. These trends are considered in light of the 4 Cs (as detailed in KCSIE), a whole-school contextual safeguarding approach that informs our curriculum, safeguarding, and technical policies.

The rise of self-generative artificial intelligence has made AI tools more accessible, often allowing students unsupervised access to text- and image-generating technologies both at home and in school. These tools pose several challenges: they can deliver inaccurate or harmful information when students seek reliable sources, facilitate plagiarism, and most importantly, compromise safety. None of the major platforms offer robust safety settings for end users, and most have age restrictions of 13 or 18. While some tools may block explicit content, they can still produce inappropriate material. Schools must address both the content brought into the classroom and educate students and parents on the responsible use of these tools at home. Furthermore, AI has increased the creation of sexualized images and deepfake videos, which, though not real, can severely harm a young person's emotional wellbeing and safety. Such content can also be weaponized to blackmail, humiliate, or abuse individuals. Alarmingly, the Internet Watch Foundation has reported a troubling rise in AI-generated child sexual abuse imagery.

According to Ofcom's 'Children and Parents: Media Use and Attitudes Report 2024', YouTube remains the most popular platform among under-18s, with WhatsApp, TikTok, and Snapchat seeing further growth, particularly with WhatsApp now open to users aged 13 and older. Children aged 3-17 are spending an average of 3 hours and 5 minutes online daily, and 40% of parents report difficulty in managing their child's screen time. Notably, 45% of children aged 8-11 feel their parents' screen time is excessive, highlighting the importance of adults modelling healthy digital habits.

Despite the 13+ age requirement for most social media platforms, 51% of children under 13 are using them, with 40% admitting to using fake ages. This exposes them to content inappropriate for their age and increases the risk of harm. Surprisingly, over one-third (36%) of parents of children aged 3-17 would permit their child to have a profile on sites or apps before they meet the age requirement. As a school, we recognize that many of our students are using these platforms regardless of age limits. We aim to promote best practices while acknowledging the reality many of our students face.

Particularly striking is the fact that 25% of children aged 3-4 already have their own mobile phone, with this figure rising to over 90% by the end of primary school. Most of these devices lack proper safety controls or restrictions to prevent harm or access to inappropriate material. Even children as young as 3-6 years old are being coerced into creating "self-generated" sexual content, despite seemingly using devices safely at home, and children aged 7-10 remain the fastest-growing group for this type of child sexual abuse material.

There is also a growing trend of children and young people using social media platforms such as Snapchat as their primary source of news, often without verifying the information or the credibility of the influencers sharing it. The rapid spread of misinformation surrounding the Southport attack in August 2024 is a prime example of this. False claims about the assailant led to Islamophobic and racist violence, rioting, and looting across England. Despite efforts by the police and national media to correct the false information, social media platforms like X amplified the misinformation, which reached millions of views and was promoted by high-profile users with large followings.

Another serious safeguarding concern involves parents filming interactions with school staff outside the school gates and posting them on social media, which poses a risk to children and the wider school community.

Cybersecurity has become a critical aspect of safeguarding and is now emphasized in KCSIE. Unfortunately, the education sector remains a key target for cyberattacks. The Cyber Security Breaches Survey 2024 reported an increase in school-related attacks, with 71% of secondary schools and 52% of primary schools experiencing breaches or attacks in the past year.

11.9 Use of generative AI

At Bushbury Hill Primary School, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE’s guidance on this.
In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.
- All staff requests for unblocking need to be passed to Mrs C Price (Online Safety Lead) who will then seek approval from Mrs C Underwood (Headteacher/DSL).
- Pupils will not be granted access to access the use of AI for completing their work. They will be made aware of the pros and cons of AI within Computing, Online Safety and PSHE.

- AI features within our Computing, Online Safety and PSHE lessons. Children will be taught about the varying suitability of generative AI. It is important that all pupils are taught the necessary skills to effectively and safely use AI whilst understanding the pros and cons in doing so. Children need to understand how AI works and the importance of how AI is only as useful as the model it learns from.
- Training sessions for Staff and parents will be led by Patrick Flynn and Charlie Price over the course of the year to ensure everyone is aware of the pros and cons of generative AI.

As a school we have agreed that staff will never enter personal or sensitive information into an AI tool. Our school may also be targeted by fraudulent emails, such as 'phishing' attacks, which are often AI-generated and very convincing. Look out for the following signs:

- Email addresses that don't match the contact details you have on file
- Poor spelling and grammar, including American spellings, or an overly formal tone
- Messages demanding urgent, time-sensitive action
- Suspicious links, e.g. containing strings of numbers
- Generic introductions (e.g. Dear Sir or Madam)
- Report any suspicious emails to our data protection officer (DPO),

In school, we allow use of co-pilot as we are a Microsoft school. ChatGPT needs to be used with careful consideration to ensure that no personal or sensitive information is entered as it is a world-wide network and outside the restrictions of Microsoft. If staff are using ChatGPT or Co-pilot they will not do this with the children present due to the risks that may be associated with the responses.

As a school staff will be allowed to use AI to cut down on some workload. For example, it could help you:

- Create a comment bank to use when writing reports
- Come up with ideas for charity fundraising activities
- Write quiz questions to check pupils' knowledge

Responding to an Online Safety Concern Flowchart

Key Local Contacts

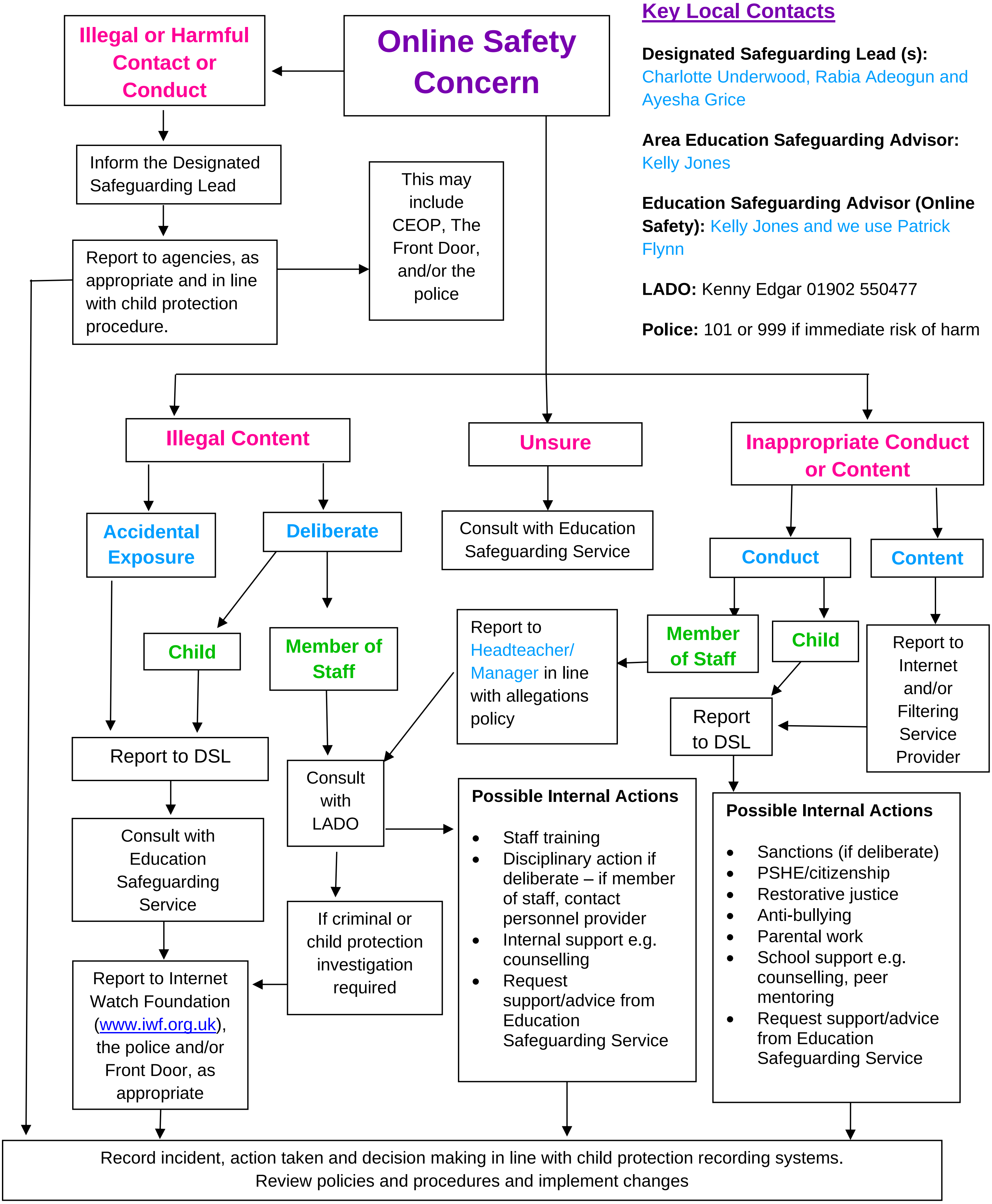
Designated Safeguarding Lead (s): Charlotte Underwood, Rabia Adeogun and Ayesha Grice

Area Education Safeguarding Advisor: Kelly Jones

Education Safeguarding Advisor (Online Safety): Kelly Jones and we use Patrick Flynn

LADO: Kenny Edgar 01902 550477

Police: 101 or 999 if immediate risk of harm



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

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

This may include CEOP, The Front Door, and/or the police

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

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

Consult with LADO

If criminal or child protection investigation required

Unsure

Consult with Education Safeguarding Service

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
- Request support/advice from Education Safeguarding Service

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
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

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

Useful Links

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

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

- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org