PORTSMOUTH AND WINCHESTER DIOCESAN ACADEMIES TRUST

Online Safety (E Safety) Policy

Date Agreed: **January 2021**

Review Date: **January 2022**

Signed: _____

Chair of Governors

St Blasius C of E Primary Academy
Portsmouth and Winchester Diocesan Academies Trust

Online Safety (E Safety) Policy

Revision Record

Revision No.	Date Issued	Prepared By	Approved	Comments
1	January 2020	CW	LGB	Reviewed policy
2	September 2020	CW	LGB	Staff name changes
3	January 2021	CW	LGB	Reviewed policy added link to KCSIE
4				
5				

Online Safety (E Safety) Policy

1. Creating an Online Safety Ethos

1.1. Aims and policy scope:

- St Blasius C of E Primary Academy believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- St Blasius C of E Primary Academy identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.
- St Blasius C of E Primary Academy has a duty to provide the academy community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the academy's management functions. The academy also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

1.2 The breadth of issues classified within online safety is considerable, but can be 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 behaviour that increases the likelihood of, or causes, harm *(Keeping Children Safe in Education* https://www.gov.uk/government/publications/keeping-children-safe-in-education--2*)*

- The purpose of St Blasius C of E Primary Academy online safety policy is to:
  - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the academy is a safe and secure environment.
  - Safeguard and protect all members of the academy community online.
  - Raise awareness with all members of the academy community regarding the potential risks, as well as benefits of technology.
  - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the local governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the academy (collectively referred to as 'staff' in this policy), the Portsmouth and Winchester Diocesan Academies Trust, as well as children and parents/carers.
- This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with academy issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant academy policies including (but not limited to) child protection/safeguarding, anti-bullying, behaviour, data security, image use, acceptable Use Policies, confidentiality, and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Relationships and Sex Education (RSE).

1.3 Key responsibilities of the community

1.3.1 Key responsibilities of the academy leaders and local governors are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the academy community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement (the Trust provide a staff questionnaire to assist this).
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the academy (the Trust provide a checklist to assist this).
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety, including adopting those provided by the Trust
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the academy community and ensuring that the filtering and academy network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole academy curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and reviewing on at least a termly basis, online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the academy community to access regarding online safety concerns, including internal, local and national support.
- To work with and support technical staff in monitoring the safety and security of the academy's systems and networks.
- To ensure that the Designated Safeguarding Lead (DSL) Nicki Mobley works in partnership with the online safety/e-Safety lead. (**if they are not the same person**)

1.3.2 Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the academy lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the academy's safeguarding recording structures and mechanisms. This should be reviewed by the Local Governing Body on a termly basis.
- Monitor the academy online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the academy management team, Local Governing Body and other agencies as appropriate.
- Liaising with the Portsmouth and Winchester Diocesan Academies Trust and other local and national bodies as appropriate or required.
- Amend, update and ensure the adoption of online safety policies, including Acceptable Use Policies (AUPs) and other procedures on an annual basis with stakeholder input. Trust models must be used where provided.
- Ensuring that online safety is integrated with other appropriate academy policies and procedures.

- Leading an online safety team/group with input from all stakeholder groups.
- Meet at least termly with the Local Governing Body member who has the lead responsibility for online safety.

1.3.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading the academy Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of academy systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities, rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible and teaching is specifically, on at least a termly basis.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.3.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on academy-owned devices.
- Ensuring that the academy's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the academy's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the internet provider and/or Portsmouth and Winchester Diocesan Academies Trust as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the academy's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 Key responsibilities of children are:

- Contributing to the development of online safety policies.

- Adhering to the academy Acceptable Use Policies (AUPs).
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6. Key responsibilities of parents and carers are:

- Reading the academy Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the academy in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the academy, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the academy online safety policies.
- Using academy systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the academy website

- The academy will ensure that information posted on the academy website meets the requirements as identified by the Department for Education. Leaders will act promptly on feedback/checks provided by the Trust and Local Governors will monitor compliance on at least a termly basis.
- The contact details on the website will be the academy address, email and telephone number. Staff or pupils' personal information will not be published.
- The Principal will take overall editorial responsibility for online content published by the academy and will ensure that content published is accurate and appropriate.
- The academy website will comply with the academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Pupils work will only be published with their permission or that of their parents/carers.
- The administrator account for the academy website will be safeguarded with an appropriately strong password.
- The academy will post information about safeguarding, including online safety on the academy website.

2.2 Publishing images and videos online

- The academy will ensure that all images are used in accordance with the academy image use policy.
- In line with the academy's image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- Pupils may only use academy provided email accounts for educational purposes.
- All appropriate members of staff are provided with a specific academy email address to use for any official communication.
- The use of personal email addresses by staff for any official academy business is not recommended.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the academy community must immediately tell the designated safeguarding lead and/or Principal if they receive offensive communication and this should be recorded in the academy online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Whole class or group email addresses may be used for communication outside of the academy.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on academy headed paper would be.
- Academy email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Appropriate and safe classroom use of the internet and associated devices

- The academy's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Pupils will use age and ability appropriate tools to search the Internet for content. Pupils will be guided by the teacher to sites suitable for their use.
- Internet use is a key feature of educational access and all children will receive at least termly age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole academy curriculum.
- The academy will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All academy owned devices will be used in accordance with the academy Acceptable Use Policy and with appropriate safety and security measure in place. Mobile device management software is used. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The academy will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole academy requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of St Blasius C of E Primary Academy community and exist in order to safeguard both the academy and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chat rooms, instant messenger and many others.
- All members of the academy community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the academy community.
- All members of the academy community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The academy will control pupils and staff access to social media and social networking sites whilst on site and using academy provided devices and systems.
- The use of social networking applications during academy hours for personal use is/is not permitted.
- Any concerns regarding the online conduct of any member of the academy on social media sites should be reported to the academy leadership team and will be managed in accordance with existing academy policies such as disciplinary, anti-bullying, allegations against staff, protected disclosures, behaviour and child protection.
- Any breaches of academy policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant academy policies, such as disciplinary, anti-bullying, allegations against staff, protected disclosures, behaviour and child protection.

3.2. Official use of social media

Relevant for all academies who use social media officially as a communication channel.

- Official use of social media sites by the academy will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official academy social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use academy provided email addresses to register for and manage official academy approved social media channels.
- Members of staff running official academy social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official academy social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official academy social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

- Official social media use by the academy will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official academy social media sites/channels in accordance with the academy image use policy and the permission of parents/carers.
- Information about safe and responsible use of academy social media channels will be communicated clearly and regularly to all members of the academy community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the academy website and take place with written approval from the leadership team.
- The leadership team must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and pupils will be informed of any official academy social media use, along with expectations for safe use and academy action taken to safeguard the community.
- St Blasius C of E Primary Academy official social media channels are:
    - PTA Facebook page
- Public communications on behalf of the academy will, where possible, be read and agreed by at least one other colleague.
- The academy social media account will link back to the academy website and/or Acceptable Use Policy to demonstrate that the account is official.
- The academy 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.

3.3.1 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the academy, then they are requested to be professional at all times and remember that they are an ambassador for the academy and the Portsmouth and Winchester Diocesan Academies Trust.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the academy.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within academy, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the academy social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the academy unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the academy online safety (e-Safety) lead and/or the Principal of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via academy communication channels.
- Staff using social media officially will sign the academy social media Acceptable Use Policy before official social media use will take place.

3.3.2 Staff personal use of social media

- Personal use of social networking, social media and personal publishing 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 the academy Acceptable Use Policy.

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/member of Leadership Team/Principal.
- If ongoing contact with pupils is required once they have left the academy roll, then members of staff will be expected to use existing alumni networks or use official academy provided communication tools.
- All communication between staff and members of the academy community on academy business will take place via official approved communication channels (*such as academy email address or phone numbers*). Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Principal/line manager.
- Any communication from pupils/parents received on personal social media accounts will be reported to the academy's designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with academy's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the academy.
- Members of staff are encouraged not to identify themselves as employees of the academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the academy and also to safeguard the privacy of staff members and the wider academy community.
- Member of staff will ensure that they do not represent their personal views as that of the academy on social media.
- Academy email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the academy's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

3.3.3 Pupils use of social media

- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the academy Acceptable Use Policy.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, academy attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the academy, where possible.
- The academy is aware that many popular social media sites state that they are not for children under the age of 13, therefore the academy will not create accounts within the academy specifically for the children.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at academy, will be dealt with in accordance with existing academy policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites and may be referred to the police and/or Children's Services.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members the academy community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the academy and covered in appropriate policies including the academy Acceptable Use Policy
- The academy recognises that personal communication through mobile technologies is an accepted part of everyday life for but requires that such technologies need to be used safely and appropriately within academy.

4.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought in to academy are the responsibility of the user at all times. The academy accepts no responsibility for the loss, theft or damage of such items. Nor will the academy accept responsibility for any adverse health effects caused by any such devices either potential or actual now or in the future.
- Mobile phones and personal devices are not permitted to be used in certain areas within the academy site such as toilets and at swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the academy community and any breaches will be dealt with as part of the academy discipline/behaviour policy.
- Appropriate members of staff will be issued with an academy email address where contact with pupils or parents/carers is required.
- All members of the academy community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the academy community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the academy will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the policies of the academy.
- Academy mobile phones and devices must always be used in accordance with the Acceptable Use Policy
- Academy mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- The academy advises that pupils do not bring mobile phones into the academy. If they are brought in to the academy, they should be switched off and left with the class teacher until the end of the academy day.
- Mobile phones or personal devices will not be used by pupils during lessons.
- If a pupil needs to contact his/her parents/carers they can ask office staff to phone them. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Phones and devices must not be taken into any 'testing' situation. Pupils found in possession of a mobile phone or personal device during a test will be reported to the Principal. This may result in the pupil's withdrawal from either that test or all tests.
- If a pupil breaches the academy policy then the phone or device will be confiscated and will be held in a secure place in the academy office until the end of the day. Mobile phones and devices will be released to parents/carers in accordance with the academy policy.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-exiting relationships which could compromise this must be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the academy policy then disciplinary action may be taken.
- 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 then the police will be contacted and allegations will be responding to following the allegations against staff policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the academy's policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the academy image use policy.
- The academy will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- St Blasius C of E Primary Academy is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the academy leadership team will ensure that appropriate risk assessments are carried out before use in the academy is permitted.
- The academy will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The academy uses RM SafetyNet to provide the school filtering service which has been designed to educational objectives approved by RM SafetyNet. In accordance with KCSIE 2020, the UK Safer Internet Centre has published guidance on what "appropriate" might look like here: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring
- The academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an academy computer or device.
- The academy will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the academy's leadership team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the academy's leadership team and Local Governing Body.

5.2. Internet use throughout the wider academy community

- The academy will adopt the policies and procedures of the Portsmouth and Winchester Diocesan Academies Trust, in order to establish a common approach to online safety (e–Safety).
- The academy will provide an Acceptable Use Policy for any guest/visitor who needs to access the academy computer system or internet on site

5.3 Authorising internet access

- The academy will maintain a current record of all staff and pupils who are granted access to the academy's electronic communications.
- All staff, pupils and visitors will read and sign the Academy Acceptable Use Policy before using any academy ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Academy Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the academy community (such as with children with special education needs) the academy will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole academy, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.

- Pupils input will be sought when updating and developing academy online safety policies and practices.
- Pupils will be supported in reading and understanding the academy Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Online safety (e-Safety) will be included in the PSHE, RSE, Citizenship and Computing programmes of study as appropriate, covering both safe academy and home use.
- The pupil Acceptable Use expectations and e-safety posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support may be used to complement and support the academy's internal online safety (e-Safety) education approaches.

6.2 Engagement and education of children and young people who are considered to be vulnerable

- St Blasius C of E Primary Academy is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

6.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of academy safeguarding practice. It will also be available to download on the academy website.
- To protect all staff and pupils, the academy will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and regular staff training in safe and responsible Internet use, both professionally and personally, will be provided for members of staff, which is integrated, aligned and considered as part of the overarching safeguarding approach.
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of academy could have an impact on their role and reputation within academy and as part of the Portsmouth and Winchester Diocesan Academies Trust. Civil, legal or disciplinary action could be taken if they are found to bring the profession, academy or multi-academy trust into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- St Blasius C of E Primary Academy recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the academy online safety (e-Safety) policy and expectations in newsletters, letters, the academy prospectus and on the academy website.
- A partnership approach to online safety at home and at academy with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

- Parents will be requested to read online safety information as part of the Home School Agreement and encouraged to role model positive behaviour for their children online.
- Parents will be encouraged to read the academy Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats, as requested.

7. Managing Information Systems

7.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Full information regarding the academy's approach to data protection and information governance can be found in the academy's data protection policy.

7.2 Security and Management of Information Systems

- The security of the academy information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the academy's network will be regularly checked.
- The computing coordinator/network manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the academy network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access academy systems. Members of staff are responsible for keeping their password private.
- From year 1, all pupils are provided with their own unique username and private passwords to access academy systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff to change their passwords at least half termly and pupils to change their passwords annually.

7.3 Filtering Decisions

- The academy's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- The academy uses educational filtered secure broadband connectivity through RM SafetyNet which is appropriate to the age and requirement of our pupils.
- The academy uses RM SafetyNet filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The academy will ensure that age and ability appropriate filtering is in place whilst using academy devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.

- The academy will be careful that “over blocking” does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- The academy will work with the broadband/filtering provider to ensure that filtering policy is continually reviewed.
- The academy will have a clear procedure for reporting breaches of filtering which all members of the academy community (all staff and all pupils) will be made aware of. All breaches are to be reported to the E-Safety lead.
- If staff or pupils discover unsuitable sites, the URL will be reported to the academy Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The Academy filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- All changes to the academy filtering policy will be logged and recorded.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the academy believes is illegal will be reported to appropriate agencies such as the Police or CEOP immediately.

7.4 Management of applications (apps) used to record children’s progress e.g. Tapestry

- The Principal is ultimately responsible for the security of any data or images held of children.
- Personal staff mobile phones or devices will not be used for any apps which record and store children’s personal details, attainment or photographs.
- Only academy issued devices will be used for apps that record and store children’s personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

- All members of the academy community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded and dealt with in line with child protection policies and procedures.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Hampshire Safeguarding Children Board thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the academy’s complaints procedure and disciplinary/behaviour policy as appropriate.
- Complaints about online bullying will be dealt with under the academy’s anti-bullying policy and child protection policy.
- Any complaint about staff misuse will be referred to the Principal.
- Any allegations against a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer) in accordance with the allegations of abuse against staff policy.
- Pupils, parents and staff will be informed of the academy’s complaints procedure and it will be made available on the academy website.
- Staff will be informed of the protected disclosures (whistleblowing) procedure.
- All members of the academy community will need to be aware of the importance of confidentiality and the need to follow the official academy procedures for reporting concerns.

- All members of the academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the academy community.
- The academy will manage online safety (e-Safety) incidents in accordance with the academy discipline/behaviour or child protection policy where appropriate.
- The academy will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the academy will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the academy will contact the Hants Direct or Hampshire Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Hampshire Police.
- If the academy is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Hants Direct.
- If an incident of concern needs to be passed beyond the academy then the concern will be escalated to the Hants Direct and the Portsmouth and Winchester Diocesan Academies Trust to communicate to other academy and school settings as deemed appropriate.
- Parents and children will need to work in partnership with the academy to resolve issues.
  Further guidance on e-safety and keeping children safe online can be found here:
  http://www.nen.gov.uk/
  www.thinkuknow.co.uk
  www.disrespectnobody.co.uk
  www.saferinternet.org.uk
  www.internetmatters.org
  www.pshe-association.org.uk
  www.educateagainsthate.com
  www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Links to other policies

This policy has links to several other policies including: Child Protection Policy & safeguarding procedures, Acceptable Use Policies, Visitors Policy & Visiting Speakers Agreement, and Tackling Extremism & Radicalisation

The following national guidelines should also be read when working with this policy:

- Prevent Strategy HM Government 2015
- Keeping Children Safe in Education DfE
  https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Working Together to Safeguard Children DfE 2015
- Promoting fundamental British values as part of SMSC in schools 2014

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

- St Blasius C of E Primary Academy ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").
- The academy will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The academy views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead Nicki Mobley
- If the academy are made aware of incident involving indecent images of a child the academy will:
    - Act in accordance with the academy's child protection policy and the relevant Isle of Wight Safeguarding Children's Partnership' policies.
    - Immediately notify the designated safeguarding lead.
    - Store the device/hard copy evidence (e.g. printed photos) securely.
    - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Implement appropriate sanctions in accordance with the academy's behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the academy is implementing best practice and the leadership team will review and update any management procedures where necessary.
- The academy will not view any images unless there is a clear need or reason to do so i.e. if requested to by Children's Social Care/Police.
- The academy will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the academy network or devices then the academy will take action to block access to all users and isolate the image.
- The academy will need to involve or consult the police if images are considered to be illegal.
- The academy will take action regarding indecent images, regardless of the use of academy equipment or personal equipment, both on and off the premises.
- The academy will ensure that all members of the community are aware of sources of support.

9.2. Responding to concerns regarding Online Child Sexual Abuse

- St Blasius C of E Primary Academy will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The academy will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The academy views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead Nicki Mobley
- If the academy is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Hants Direct and/or Hampshire Police.
- If the academy are made aware of incident involving online child sexual abuse of a child then the academy will:

- Act in accordance with the academy's child protection policy and the relevant Isle of Wight Safeguarding Children's Partnership' policies.
- Immediately notify the designated safeguarding lead.
- Store any device/hard copy evidence (e.g. printed photos) securely.
- Immediately inform Hampshire police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate, the academy will involve and empower children to report concerns regarding online child sexual abuse
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the academy is implementing best practice and the academy leadership team will review and update any procedures where necessary.

- The academy will take action regarding online child sexual abuse regardless of the use of academy equipment or personal equipment, both on and off the academy premises.
- The academy will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools or academies are believed to have been targeted then the academy will seek support from Hants Direct to enable other schools and academies to take appropriate action to safeguarding their community.
- The academy will ensure that the Click CEOP report button is visible and available to pupils and other members of the academy community, for example including the CEOP report button the academy website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- St Blasius C of E Primary Academy will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- The academy will take action regarding the Indecent Images of Children (IIOC) regardless of the use of academy equipment or personal equipment, both on and off the premises.
- The academy will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the academy is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Hants Direct and/or Hampshire Police.

- If the academy are made aware of Indecent Images of Children (IIOC) then the academy will:
  - Act in accordance with the academy's child protection and policy and the relevant Hampshire Safeguarding Child Boards procedures.
  - Immediately notify the academy Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Hampshire police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the academy are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the academy will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.

- Inform the LADO to provide support for this situation.

- If the academy are made aware that indecent images of children have been found on the academy's electronic devices then the academy will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

- If the academy are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the academy, then the academy will:
  - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the academy protected disclosures (whistleblowing) procedure.
  - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the academy's managing allegations of abuse against staff policy.
  - Follow the appropriate academy policies regarding conduct.

9.4. Responding to concerns regarding radicalisation or extremism online

- Every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups. The academy will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in the academy and that suitable filtering is in place which takes into account the needs of pupils. RM SafetyNet filters all extremist content and cannot be changed by the academy.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the academy child protection and tackling extremism and radicalisation policies. **See The Prevent Duty for further information and guidance:** https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

9.5. Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the academy community will not be tolerated. Full details are set out in the academy policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the academy community affected by online bullying.
- If the academy is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through Hants Direct and/or Hampshire Police.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The academy will take steps to identify the bully where possible and appropriate. This may include examining academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the academy to support the approach to cyberbullying and the academy's e-Safety ethos.
- Sanctions for those involved in online or cyberbullying may include:
  - Those involved will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at the academy for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the academy's anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.