St Benet's RC VA Primary School

ST. BENET'S

Roman Catholic Primary School

Online Safety Policy

Date of Implementation: Autumn 2025

Date of Review: July 2026

Policy Aims

- This online safety policy has been written by St. Benet's RC VA Primary, involving staff, learners and parents/carers, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2025, Early Years and Foundation Stage 2017 and 'Working Together to Safeguard Children' 2023.
- The purpose of this online safety policy is to:
  - Safeguard and protect all members of St Benet's community online
  - Identify approaches to educate and raise awareness of online safety throughout the community o 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 use when responding to online safety concerns.
- St Benet's RC VA Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

  o **Content:** being exposed to illegal, inappropriate or harmful material

  o **Contact:** being subjected to harmful online interaction with other users**.**

  o **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

1. **Policy Scope**

- St Benet's RC VA Primary School believes 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.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use offsite.

a. **Links with other policies and practices**

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of Conduct
- Behaviour for Learning policy

o Child Protection/Safeguarding policy

2. **Monitoring and Review**

- Technology in this area evolves and changes rapidly. St Benet’s RC VA Primary School will review this policy at least annually or following any national or local policy requirements, any child protection concerns or any changes to the 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 and recorded on CPOMs.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

3. **Roles and Responsibilities**

- The Designated Safeguarding Lead (DSL), **Mrs A Goodwin**, has lead responsibility for online safety. (***Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.)
- *St Benet’s* recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

a. **The leadership and management team will:**

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.

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

b. **The Designated Safeguarding Lead (DSL) will:**

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the setting's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant 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 SEND face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting's management team and Local Governing Committee as well as meeting with lead governor's around this.

c. **It is the responsibility of all members of staff to:**

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Embed online safety education in curriculum delivery, wherever possible (at least one lesson per half-term, as well as Safer Internet day).

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

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

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others, both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

e. **It is the responsibility of parents and carers to:**

- Read the acceptable use 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.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. **Safer Use of Technology**

a. **Classroom Use**

- St Benet's RC VA Primary School uses a wide range of technology.
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home, this includes AI programs and apps, such as Copilot.
- Supervision of learners will be appropriate to their 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 learners' age and ability.

  - **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 learners' age and ability.
  - **Learners in residential provision / school events**
    - During school residential visits, pupils are not allowed to access digital devices. Staff are reminded about appropriate use of such devices.
- **Artificial Intelligence**

  Staff will ensure safe use of AI in preparing resources and materials for lessons. Children will not be asked to use it through curriculum time. Please refer to our Artificial Intelligence guidance for detailed policy and procedure.

b. **Managing Internet Access**

• All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

c. **Filtering and Monitoring**

i **Decision Making**

- St Benet's RC VA Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed through discussion with stakeholders.
- 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.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate – weekly Smooth wall email reports and timely alerts.
- 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.

ii Filtering

- We use a filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, blogging and sites of an illegal nature. School is also aware of the filtering detecting other safeguarding issues, such as self- harm, serious violent crime or issues with county lines grooming.
- We work with One IT to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
  - Turn off monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Durham Police or CEOP.

iii Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - The school Smooth wall provides reports about usage that could potentially indicate an issue which requires further investigation. Alerting e-mails are sent to The Headteacher who then takes appropriate action.
- If a concern is identified via monitoring approaches we will:
  - List how concerns will be responded to e.g. DSL or deputy will respond in line with the child protection policy.
- 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.

d. 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.

o Full information can be found in our Data Protection policy.

e. **Security and Management of Information Systems**

- We take appropriate steps to ensure the security of our information systems, including:
  - o Virus protection being updated regularly.
  - Regularly checking files held on our network.
  - The appropriate use of user logins and passwords to access our network.
  - Specific user logins and passwords updated regularly for all.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

f. **Password policy**

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From Year 1 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

5. **Social Media**

Please also refer to our Acceptable Use Policy/ Staff Code of Conduct.

a. **Staff Personal Use of Social Media**

- The safe and responsible 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.

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 setting.

  o 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 sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

  o Setting the privacy levels of their personal sites.
  o Being aware of location sharing services.

  - o Opting out of public listings on social networking sites.
  - o Logging out of accounts after use.
  - o Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff should not identify themselves as employees of St Benet's RC VA Primary School on their personal social networking accounts.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and 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.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
- Any communication from learners and parents received on personal social media accounts will be reported to the headteacher.

c. **Learners' Personal Use of Social Media**

- Learners will be advised:
  - To consider the benefits and risks of sharing personal details 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 responsible adult's permission and only 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 both within the setting and externally.

6. **Use of Personal Devices and Mobile Phones**

• St Benet's RC VA Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

a. **Expectations**

- All use of personal devices (including but not limited to; tablets, and ‘smart’ watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- All members of St Benet’s RC VA 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.
- All members of St Benet’s RC VA Primary School community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the discipline policy.

b. **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.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place 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 permission has been given by the headteacher, such as in emergency circumstances.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting learners or parents and carers unless instructed to do so by the headteacher. In these circumstance staff should ensure that caller ID is withheld.

  If a member of staff breaches our policy, action will be taken in line with our code of conduct and whistle blowing policy
  o 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, the police will be contacted.

c. **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.
- St Benet's RC VA Primary School expects learners' personal devices and mobile phones to be…
  - kept in a secure place, switched off, kept out of sight during lessons
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Mobile phones and devices that have been confiscated will be released to parents or carers 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.

d. **Visitors' Use of Personal Devices and Mobile Phones**

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) headteacher of any breaches our policy.

7. Procedures for Responding to Specific Online Incidents or Concerns

a. **Online Sexual Violence and Sexual Harassment between Children**

- St Benet's RC VA Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- St Benet's RC VA 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

between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

- 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 online sexual violence and sexual harassment, we will follow our safeguarding procedures and report this to the relevant bodies.
-

Youth Produced Sexual Imagery ("Sexting")

- St Benet's RC VA Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- 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 images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

  If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

b. **Online Child Sexual Abuse and Exploitation**

- St Benet's RC VA Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- If made aware of incident involving online child sexual abuse and we will:
  - Act in accordance with our child protection policies.
  - If appropriate, store any devices involved securely.
  - Make a referral to safeguarding team and immediately inform the police via 101, or 999 if a child 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.
  - 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately.

c. **Indecent Images of Children (IIOC)**

- 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 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 Police and/or the Education Safeguarding Team.

- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as Police or the LADO.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

  o Ensure that the DSL (or deputy) is informed.
  - 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:

  o Ensure that the DSL (or deputy) is informed.
  - 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 First Contact

    - 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.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the headteacher is informed in line with our managing allegations against staff policy and secure any devices.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.

d. **Child Criminal Exploitation – Including County Lines**

• All staff need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in the schools safeguarding policy.

e. **Cyberbullying**

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St Benet's RC VA Primary.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

f. **Online Hate**

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St Benet's RC VA Primary School and will be responded to in line with existing policies, including 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 First Contact or Police

g. **Online Radicalisation and Extremism**

- 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 child/parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our policies.
- 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.