St Barnabas

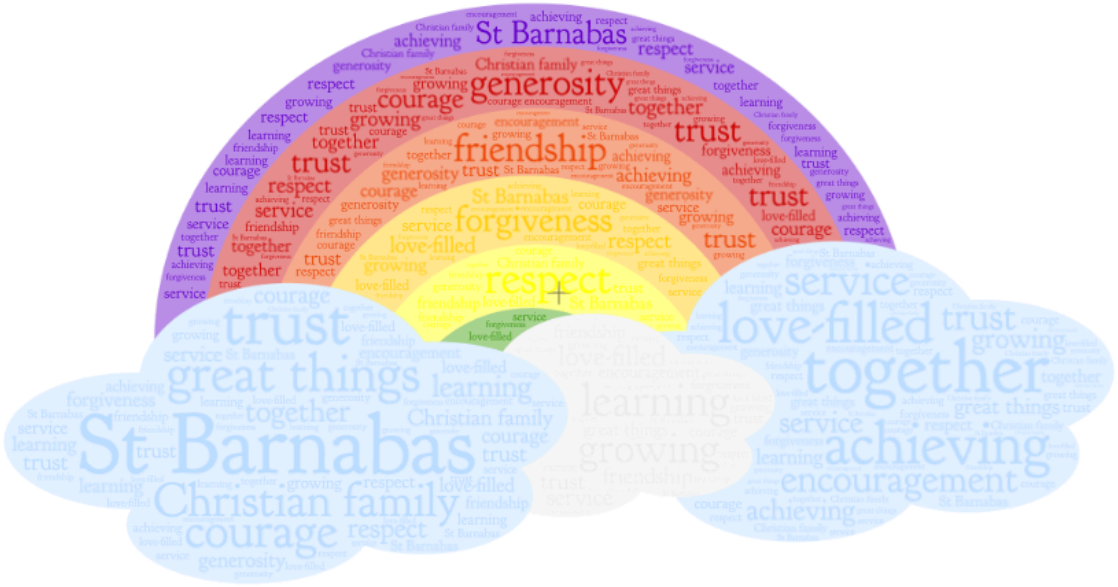
Church of England Primary Academy

A member of CTDARI

Our Vision: 'Achieving great things through learning and growing together in a love-filled Christian family'

'That they shall have life, life in all its fullness!' John 10:10

Online Safety Policy



Online Safety Lead: Emma Wilkinson

Headteacher: Mrs Becky Ham

Online Safety Link Governor: Beth Speak

1. Aims

St Barnabas CE Primary Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
3. Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on: Teaching online safety in schools, Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff, Relationships and sex education and Searching, screening and confiscation
It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The local governing committee

The local governing committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will discuss online safety, and monitor online safety logs (which will be recorded on my concern) as provided by the deputy safeguarding lead. The link governor will oversee online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see ICT Acceptable use policy)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead and the designated deputy safeguarding leads

Details of the school's DSL (and deputy DSL) are set out in our child protection and safeguarding policy and on our school website https://www.stbarnabasdarwen.co.uk/key-information/safeguarding

The DSL and Deputy DSL takes responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (on my concern) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on my concern and dealt with appropriately in line with the school behaviour policy and safeguarding policy.
- Updating and delivering staff training on online safety (logged on Every)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitor the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are reported to the DSL or deputy DSL's

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems (see ICT Acceptable use policy), and ensuring that pupils follow the school's terms on acceptable use (by signing the home school agreement)
- Working with the DSL's to ensure that any online safety incidents are logged (on my concern) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately and logged onto myconcern
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (on the home school agreement via a google form)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? – UK Safer Internet Centre
    - Hot topics – Childnet International
    - Parent resource sheet – Childnet International
    - Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

Relationships education and health education in primary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in Computing and PSHE lessons.

If appropriate, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

St Barnabas CE Primary Academy will raise parents' awareness of internet safety on Class Dojo, and in information via our website https://www.stbarnabasdarwen.co.uk/parents/useful-links/online-safety. This policy will also be shared with parents. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Deputy DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will use aspects of the curriculum to cover cyber-bullying. This includes during personal, social, health and economic (PSHE) education lessons.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (recorded on Every).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work

with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Any devices that are brought into school are locked away and children do not have access to them throughout the school day.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Cyber-attacks

St Barnabas is a Google school and the IT manager is responsible for conducting a full security check. All staff have been directed to the National Cyber Security Centre document 'Cyber Security in school: practical tips for everyone working in education'. St Barnabas follows the basic principles of good cyber security. These include powerful passwords, watching out for phishing, the correct use of USB and pen drives and ensuring all devices have passcodes and software is kept up to date.

All staff members will take appropriate steps to ensure their devices remain secure. At St Barnabas, we use Google drive to ensure documents remain in a safe online space. Steps that need to be taken include, but are not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

8. Online abuse and exploitation

Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL or Deputy DSL and dealt with in line with the Child Protection and Safeguarding Policy.

9. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see ICT Acceptable use policy and home school agreement).
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
The ICT Manager will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

10. Staff using work devices outside school

Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the ICT Manager or DSL and Deputy DSL.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, incidents are recorded on my concern and the safeguarding leads are notified. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the (ICT acceptable use policy). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The academy trust and school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Staff are also directed to our online safety page on our school website.

By way of this training, all staff will be made aware that:
Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or

videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our safeguarding and child protection policy.

13. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety on my concern. This is then monitored by the DSL and deputy DSL. This policy will be reviewed every year by the online safety leader. At every review, the policy will be shared with the governing board.

E WILKINSON

ONLINE SAFETY LEADER

JULY 2024