St Barnabas Church of England Infant School

Online Safety Policy

Committee Person(s) Responsible:

Senior Leadership Team

Review date: September 2024

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of school ICT systems, both in and out of the school.

Behaviour - Our Vision

At St Barnabas, we believe all children should have a safe and happy place to learn. To do this, we aim for all children to demonstrate positive behaviour at all times, both in and out of the classroom. Our aim is for children to manage their own behaviour and to be responsible for their own actions. Our school is committed to creating a caring, secure and stimulating environment in which individuals feel respected, included and valued. We believe this gives individuals the opportunity to reach their full potential emotionally, socially and academically. Because we promote a climate of kindness and want the best for each and every child, we expect everyone in our school community to act as role models promoting our core values:

- Kindness: 'Show kindness to my family because I have shown kindness to you.' Joshua 2:12
- Love: 'You shall love your neighbour as you love yourself.' Mark 12:31
- Forgiveness: 'Be kind to one another, tender hearted, forgiving one another, as God in Christ forgave you.' Ephesians 4:32
- Honesty: 'Walk with integrity, be righteousness, speak with truth.' Psalm 15:2
- Respect: 'Show respect to everyone.' Peter 2:17

These values are promoted consistently across the school and children are taught how to demonstrate these values in and out of school. All classrooms have the values displayed and they are regularly referred to as part of the children's learning. Children should always be praised for demonstrating the core values. At St Barnabas, we strive for children to demonstrate positive behaviour that will contribute to success in school and later on in adult life. Our values guide us through daily life at St Barnabas; we strive for all members of the school community to display these values at all times.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; child criminal exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. It is recognised that an effective whole academy approach to online safety empowers an academy to protect and educate the whole academy community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk as set out in KCSIE:

- content: being exposed to illegal, inappropriate or harmful content; for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti- Semitism, radicalisation and extremism
- contact: being subjected to harmful online interaction with other users; for example 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

- conduct: online behaviour that increases the likelihood of, or causes harm; for example making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nude and seminude and/or pornography, sharing other explicit images and online bullying), and

- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If the Academy feels their children or staff are at risk, they should report it to the Anti Phishing Working Group (https://apwg.org/).

Bullying

"Bullying behaviour abuses an imbalance of power to repeatedly and intentionally cause emotional or physical harm to another person or group of people. Isolated instances of hurtful behaviour, teasing or arguments between individuals would not be seen as bullying." (Torfaen definition 2008).

Bullying is:

- Deliberately hurtful or threatening behaviour.
- It is premeditated and usually forms a pattern of behaviour rather than an isolated incident.
- It involves dominance of one pupil by another, or group of others. Bullying can be:
- Emotional: when a person is deliberately or excludes another person by being overtly nasty or unkind. An example of emotional bullying is encouraging people not to play with somebody or making fun of somebody.
- Other examples are tormenting (e.g. hiding books, threatening gestures) and ridicule.
- Physical: a deliberate physical act which results in injury or hurt feelings. Examples include punching, slapping or kicking or any use of violence or threatened violence.
- Psychological: This is a very complex form of bullying which involves deliberate acts which cause fear or anxiety in another person.

Bullying can also be:

- Racist: racial taunts, graffiti, gestures
- Sexual: unwanted physical contact or sexually abusive comments
- Homophobic: because of, or focussing on, the issue of sexuality
- Verbal: name-calling, sarcasm, spreading rumours, teasing
- Religious: related to religious beliefs and practices
- Cultural: related to cultural beliefs and practices
- Cyber: all areas of internet, such as email & internet chat room misuse; mobile threats by text messaging & calls; misuse of associated technology , i.e. camera & video facilities

The school works hard to ensure that all pupils and parents know the difference between bullying and simply "falling out".

Actions to Tackle Bullying

St Barnabas Endowed CE Junior Academy is a 'telling' school. Pupils are told that they must report any incidence of bullying to an adult within school when another pupil tells them that they are being bullied or if they see bullying taking place. It is their responsibility to report their knowledge to a member of staff. For more information, please read our Anti-Bullying Policy.

Cyberbullying

Cyber bullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology. It can take many forms, but can go even further than face-to-face bullying by invading home and personal space and can target one or more people. It can take place across age groups and target pupils, staff and others. It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images. It can include messages intended as jokes, but which have a harmful or upsetting effect. Cyberbullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips via mobile phone cameras;
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Menacing or upsetting responses to someone in a chat-room; Unpleasant messages sent during instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites (e.g. Facebook) a)

At St Barnabas, cyberbullying is considered as serious as any other form of bullying. Cyber bullying issues are dealt with in an appropriate manner dependent on the severity and frequency of the issue. Cyberbullying will generally be dealt with through the school's Anti-Bullying and Behaviour policies. The Education and Inspections Act 2006 empowers headteachers to impose disciplinary penalties for inappropriate behaviour even when incidents occur off the school site. This is pertinent to incidents of cyber-bullying, or other online safety incidents, which may take place outside of the school.

Suspensions & Internal Exclusions

Instances of cyberbullying may necessitate an internal exclusion. This could mean that the child works in a different part of the school or works outside the Headteacher or Deputy Headteacher's office. The Headteacher or Deputy Headteacher will support the work by the Wellbeing and Classroom staff. The class teacher will provide accessible work for the child. The wellbeing team will work with the child to support the child's reintegration into class, either on the same day or on the next school day, during the child's own time (not in learning time). Parents will be notified if this happens and the behaviour will be logged by the Senior Leadership team on MyConcern.

Fixed-term Exclusion / Suspension

In more severe cases, a period of external exclusion may be necessary. This is dependent on the severity of

the incident and is ultimately at the discretion of the Headteacher. The school follows the Peterborough Diocese Education Trust guidance for exclusions and this can be found on the school website.

Reintegration Meeting Following Fixed-Term Exclusion / Suspension

A meeting will be arranged with parents, the Headteacher or Deputy and the child after the exclusion period ends. The aim of the meeting is to create an agreement between all parties of future expectations. Minutes of these meetings will be recorded by a member of the Senior Leadership team. The school has the right to extend the exclusion period in this meeting if the child is unwilling to comply with the expectations of the behaviour policy.

Permanent Exclusion

This extreme measure is only taken by the Headteacher and is ratified by the Academy's Governing Body. The school follows the Peterborough Diocese Education Trust guidance for exclusions and this can be found on the school website.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors

The Academy Governance Committee are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. The Governors, who will receive regular information about online safety incidents, will conduct monitoring reports regarding online safety and the implementation of this policy.

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology, online safety, health and safety and/or safeguarding.

Headteacher and Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The designated member of the senior leadership team who leads on online safety is the Deputy Headteacher. The Senior Leadership Team are responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their online safety roles. The school has a separate Bring Your Own Device (BYOD) Policy and Acceptable Use Agreement in place for staff to adhere to and the school also adheres to the principles of UKGDPR (United Kingdom General Data Protection Regulation).

ICT Systems

The company in charge of the school's ICT systems will ensure that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack and that the school meets required online safety technical requirements
- users may only access the networks and devices through a properly enforced password protection policy that enforces an appropriate level of complexity and, for staff accounts, requires passwords to be changed regularly
- the filtering policy is applied and updated on a regular basis
- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to a senior leader for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- the school has enhanced, differentiated user-level online filtering
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of systems or data
- the school infrastructure and workstations are protected by up to date virus software

Teaching and Support Staff

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support to recognise and avoid online safety risks and build their resilience. Educating pupils to take a responsible approach to online safety is essential. As such, online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

All staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices, including the use of social media
- they have read and understand the Acceptable Use Agreement
- they report any suspected misuse or problem to a senior leader for investigation / action / sanction
- all digital communications with pupils / parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety policy and acceptable use agreement
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile

devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Online safety training will form part of the regular safeguarding training for staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreement.

Pupils

Pupils are responsible for:

- using the school digital technology systems appropriately
- avoiding plagiarism and upholding copyright regulations
- reporting abuse, misuse or access to inappropriate materials and know how to do so
- understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through methods such as:

- Curriculum activities
- Letters, newsletters and the school website
- Parents sessions

- High profile events/campaigns (e.g. Safer Internet Day) Reference to the relevant web sites/publications

Data Protection

Personal data will be recorded, processed, transferred and made available in compliance with the school's Data Protection Policy. All staff receive data protection training, both through the induction programme and ongoing staff training, and are made aware of their responsibilities.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning. Pupils need to be aware of the risks associated with publishing digital images on the internet. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Pupils must not take, use, share, publish or distribute images of others without their permission.

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images.

Staff are able to take digital/video images to support educational aims as set out in the school's Data Protection Policy. Images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes. Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Permission to use photographs for purpose beyond educational assessment is sought from parents/carers and/or students and photographs may only be used if the necessary consent has been received for the purpose for which they will be used. Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Communications

The official school email service is safe, secure and monitored. When in school, or on school systems (e.g. by remote access), staff and pupils should only use the school email service to communicate. Users must immediately report to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any communication between staff, pupils or parents/carers must be professional in tone and content. These communications may only take place on official and monitored school accounts. Personal email addresses, text messaging or social media must not be used for these communications.