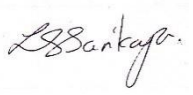
THE ST. BART'S ACADEMY TRUST

Online Safety Policy

October 2023

The St. Bart's Academy Trust

Online Safety Policy

Produced Date:	**October 2023**	
Approved by Trust Board:		**Lisa Sarikaya** Chief Executive Officer
Review Date:	**October 2025**	

Date	Section Amended	Signature

Contents

Statement of intent

St. Bart's Multi-Academy Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout our academies; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. St Bart's Multi-Academy Trust has created this policy for implementation by its academies with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

2. Roles and responsibilities

The **local governing committee** is responsible for:

- Ensuring the Designated Safeguarding Lead's (DSL) remit covers online safety.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals thereafter.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with the Trust ICT Manager and service providers.
- Ensuring that the Senior Leadership Team and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The **Principal** is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the academy policies and procedures, including in those related to the curriculum and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.

- Organising engagement with parents to keep them up-to-date with current online safety issues and how the academy is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct light-touch reviews of this policy.

The **Designated Safeguarding Lead (DSL)** is responsible for:

- Taking the lead responsibility for online safety in the academy.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the academy safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the academy's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the academy's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the academy community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the academy's provision, and using this data to update the academy's procedures.
- Understanding the filtering and monitoring processes in place at the academy.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the academy.

The **Trust ICT Manager** is responsible for:

- Providing technical support in the development and implementation of the academy's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Principal.
- Ensuring that the academy's filtering and monitoring systems are updated as appropriate.

All **staff members** are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.

- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the academy's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Designated Safeguarding Lead has overall responsibility for the academy's approach to online safety, supported by the Principal, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all academy operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum

3.1. Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the **Child Protection and Safeguarding Policy**.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Staff will follow the guidance around victim blaming ensuring that their language and actions do not imply that a pupil is partially or wholly responsible for abuse that has happened to them. All education professionals will be encouraged to think critically about the language they use and the impact that it will have.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately, the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police

against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Principal, who decides on the best course of action in line with the relevant policies, e.g. the **Staff Code of Conduct** and **Disciplinary Policy and Procedures.** If the concern is about the Principal, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members and manages concerns in accordance with relevant policies depending on their nature, e.g. the **Behaviour Policy** and **Child Protection and Safeguarding Policy**.

Where there is a concern that illegal activity has taken place, the Principal/DSL contacts the police.

The academy avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the **Child Protection and Safeguarding Policy**.

All online safety incidents and the academy's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent 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
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The academy will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the **Anti-bullying Policy / Child on Child Abuse policy**.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence

- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The academy will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The academy will respond to these incidents in line with the **Child-on-Child Abuse Policy** and the **Social Media Policy**.

The academy responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the academy premises or using academy-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the **Child-on-child Abuse Policy** and the **Child Protection and Safeguarding Policy**.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.

- Having an older boyfriend or girlfriend, usually one that does not attend the academy and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

6.1. Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

6.2. Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the academy, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the academy or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the Trust and LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Principal will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and Principal will only implement an academy-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The academy will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Principal will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology on academy -owned devices or on academy networks through the use of appropriate firewalls.

10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships Education
- PSHE
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum.

The academy recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

External visitors may be invited into the academy to help with the delivery of certain aspects of the online safety curriculum. The Principal and DSL decide when it is appropriate to invite external groups into academy and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the **Child Protection and Safeguarding Policy**.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the **Child Protection and Safeguarding Policy**.

12. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

While the academy recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the academy will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the Acceptable Use Policy.

Staff will use all smart technology and personal technology in line with the Trust Acceptable Use Policy and Staff Code of Conduct.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use personal smart devices or any other personal technology whilst on the academy site.

The academy will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The academy will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The academy works in partnership with parents to ensure pupils stay safe online at the academy and at home. Parents are provided with information about the academy's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources

15. Internet access

Staff and pupils are encouraged to explore the internet and use a range of resources for teaching and learning. This should be done in a responsible way. Rules about internet use apply equally to all staff and pupils. This helps to promote shared values within the academy.

The Wi-Fi network at the academy will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Principal.

Use of the internet is monitored to help ensure network security and promote efficient use of the available resources. Unusual volumes of traffic will be noted. If a staff member is using significant internet resources, they may be asked to explain how this promotes the academy's aims and values.

Network filtering is in place to prevent access to inappropriate sites, and there is keyword logging software that flags certain terms.

Users are expected to use the internet in accordance with UK law. Any illegal use will be dealt with through official channels, which may include the involvement of police if a crime has been committed

16. Filtering and monitoring online activity

The Trust ICT manager and Principal will ensure the academy's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. They will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the academy's safeguarding needs.

The filtering and monitoring systems the academy implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The Trust ICT Manager will ensure that:

- The firewall is checked weekly for any changes and/or updates, and that these are recorded using the inventory.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is also checked weekly to ensure that a high level of security is maintained, and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the DPO. The Trust ICT Manager will react appropriately to security threats to find new ways of managing the firewall. . The Trust ICT Manager undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Deliberate breaches of the filtering system are reported to the Principal, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the **Behaviour Policy**. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the **Disciplinary Policy and Procedure**.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The academy's network and academy-owned devices are appropriately monitored. All users of the network and academy- owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the **Child Protection and Safeguarding Policy**.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Trust ICT Manager. Firewalls are switched on at all times. The Trust ICT Manager reviews the firewalls on a regular

basis to ensure they are running correctly, and to carry out any required updates / updates have been carried out were the firewall is managed locally by a third party.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the Trust ICT Manager.

The academy understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role based. Trust academy networks are set up to provide pre agreed access levels and specific shared drive access direct from the server. These are applied to computers on first log in. Any additional access (e.g. further shares) must be communicated to the Trust ICT Manager to arrange by the Principal. Consideration on this part will ensure any potential deliberate or accidental attacks on the network are minimised.

The Trust ICT Manager will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the **Data and Cyber Security Breach Plan**.

All users will be required to change their passwords every 120 days and/or if they become known to other individuals. Pupils are responsible for remembering their passwords; however, the Trust ICT Manager will be able to reset them if necessary. The record of all usernames and passwords is encrypted. Only the Trust ICT Manager has access to this inventory if it is appropriate for a pupil to have an individual login, the Trust ICT Manager will set up their individual user account, ensuring appropriate access.

The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the academy, such as changing security settings, monitoring use, and installing software and hardware.

A multi-user account will be created for visitors to the academy, such as volunteers, and access will be filtered as per the Principal's instructions. Usernames and passwords for this account will be changed on a termly basis and will be provided as required.

Users are required to lock access to devices and systems when they are not in use.

Full details of the academy's network security measures can be found in the **Data and Cyber-security Breach Prevention and Management Plan**.

18. Emails

Access to and the use of emails is managed in line with the **Data Protection Policy**, **Acceptable Use Policy** and the **Staff Code of Conduct**.

The academy provides an email system to facilitate teaching and learning. It allows staff [and pupils] to communicate quickly with one another, and to provide a quick and easy way to deal with outside agencies on any academy business.

Staff and pupils are given approved academy email accounts and are only able to use these accounts at the academy and when doing academy-related work outside of school hours. . Personal email accounts are not permitted to be used on the academy site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to the Trust ICT Manager. The academy monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed in line with the **Data and Cyber-security Breach Prevention and Management Plan**.

19. Social networking

19.1. Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the academy. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff will not engage in inappropriate use of social networking sites including contacting pupils or their family members, accepting or inviting friend requests from pupils or their family members, or following pupils or their family members on social media, unless there is a familial relationship or in the case of parents, pre-existing relationships external to the Trust / Academy.

The Trust understands that some staff members are also parents of pupils at the Academy and therefore, may have a pre-existing relationship external to the Trust / Academy. When contacting other parents in these circumstances, doing so, staff will exercise their professional judgement and will not contact family members on social media if this would lead to a conflict of interest.

Staff will remain mindful of their use of social media and their web-based presence including written content, videos or photographs, and views expressed directly or indirectly which may bring themselves, the Trust / Academy or the Trust / Academy community into disrepute.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the academy community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. **Anti-Bullying Policy**, **Staff Code of Conduct** and **Behaviour Policy**.

19.2. Use on behalf of the academy

The use of social media on behalf of the academy is conducted in line with the Social Media Policy. The academy's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the Principal to access to the academy's social media accounts.

All communication on official social media channels by staff on behalf of the academy is clear, transparent and open to scrutiny.

20. The academy website

The Principal is responsible for the overall content of the academy website – they will ensure the content is appropriate, accurate, up-to-date and meets DfE and KCSIE requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the **Photography and Images Policy** are met.

21. Use of devices

21.1. Academy-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptop
- Tablet

Pupils are provided with academy-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

Academy-owned devices are used in accordance with the Device User Agreement. Staff and pupils are not permitted to connect academy-owned devices to public Wi-Fi networks. All academy-owned devices are password protected.. All academy-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

Academy-owned devices are reviewed on a termly basis y to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programs can be downloaded onto a device without authorisation from the Trust ICT Manager for this to be installed. Users are not permitted to install apps using the standard staff account template. Should a member of staff require an app for their staff iPad for testing purposes they can utilise their academy Apple ID to install this. Should the app then be required for other staff and/or pupils a request should be made to the Trust ICT Manager and the app will be added to the devices via the Jamf portal, where the app and associated updates can be managed.

Cases of staff members or pupils found to be misusing academy-owned devices will be managed in line with the **Disciplinary Policy and Procedure and Behaviour Policy** respectively.

21.2. Personal devices

Personal devices are used in accordance with the **Bring Your Own Device Policy**. The academy will only allow personal devices to connect to the academy network if they have first been checked by the ICT Manager. This will ensure that there is adequate virus and malware protection on the device, that the protection is up-to-date, and that the machine is free of viruses or malware. Staff members are not permitted to use their personal devices in the classrooms or during teaching lesson time. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the academy premises in line with the **Child Protection and Safeguarding Policy** and/or **Whistleblowing Procedures**. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Principal will inform the police and action will be taken in line with the Disciplinary Policy and Procedures.

Pupils are not permitted to use their personal devices whilst on the academy site. The Principal may authorise the use of mobile devices by a pupil for safety or precautionary use i.e. if travelling to and from the academy alone which will be detailed in the academy **Mobile Phone Policy**. Appropriate signage is displayed to inform visitors to the academy of the expected use of personal devices. Any concerns about visitors' use of personal devices on the academy premises are reported to the Principal.

22. Remote learning

All remote learning is delivered in line with the **Acceptable Use Policy including Remote Online Learning and Communication**.

The academy will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The academy will consult with parents prior to the period of

remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The academy will ensure that all academy-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the academy will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The academy will not be responsible for providing access to the internet off the academy premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the academy.

23. Monitoring and review

The online world is constantly changing; therefore, the DSL, Trust ICT Manager and the Principal must conduct annual light-touch reviews of this policy to evaluate its effectiveness.

The Trust will review this policy in full on a regular basis and following any online safety incidents.

THE ST. BART'S ACADEMY TRUST

St. Bart's Multi-Academy Trust
c/o Belgrave St. Bartholomew's Academy,
Sussex Place, Longton, Stoke-on-Trent, Staffordshire, ST3 4TP
www.sbmat.org T: 01782 486350

THE ST. BART'S ACADEMY TRUST

DIOCESE OF LICHFIELD
GOING FOR GROWTH

BTSA