RESPICE = PROSPICE

Blue Coat
Church of England Academy

Online Safety Policy

Date:		October 2022
Prepared by:		C. Pardoe
Ratified by the Governing Body on:		
	Signature	
Principal	DJSmith	D. J. Smith
Chair of Governors	Parker	L Parker
Review date:		October 2024

Contents

Psalm 36:7:" How priceless is your unfailing love, O God! People take refuge in the shadow of your wings."

1. Intentions

Our approach to Online Safety is based on effectively addressing the four key categories of of recognised risk relating to Online Safety.

This Online Safety Policy describes how this is done through education, routine activities and wider Policy compliance.

The 4 key categories of risk relating to Online Safety (the "Four Cs")

Content – being exposed to illegal, inappropriate or harmful content.

Contact – being subjected to harmful online interaction with other users.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance. Keeping Children Safe in Education.

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.

This policy complies with the Academy's funding agreement and articles of association.

3. Design and management of the Academy's digital estate (network).

Summary of the digital estate in relation to Online Safety:

Content

- ICT systems are protected against viruses and malware. This includes filtering and firewall settings to block access to potentially harmful or inappropriate content. Staff filtering and student filtering are set differently e.g. student users are not able to access YouTube.

Contact

- Backups are in place to mitigate risk of data loss and maximise Business Continuity, as described in the Academy's Financial Regulations documents.

Conduct

- Monitoring settings can be updated on request, for example as new slang terms become known.
- Senso logs can be regularly reviewed and any concerns reported via CPOMS.
- Teaching staff are able to use classroom device monitoring to safeguard students during lessons, and can report concerns directly to CPOMS from this platform.

Commerce

- Updates are deployed remotely and regularly.
- All staff have Microsoft A3 licensing as a minimum to ensure appropriate levels of security protection to mitigate against the risks of cyber attacks. A select group of staff have Microsoft A5 licensing representing the highest level of protection to reflect their access to sensitive data and / or finance.

- All staff have MFA (Multi Factor Authentication) enabled on their Microsoft Office accounts. For the majority of staff, this is enabled offsite only to minimise disruption to their roles onsite. Mirroring the approach to licensing, a select group of staff have MFA enabled both on and offsite. This reflects their access to sensitive data and / or finance.
- The Academy no longer uses Remote Access technology, reducing security risks through the use of cloud file storage and MIS hosted in the cloud. The link to access the MIS remotely is only made available within the Academy's native Office365 environment.
- The Strategic Lead for IT and their team conduct regular simulations of cyber attacks using Microsoft security tools. The intention is to harden colleagues' security stance on malicious links and credential harvesting, and to provide further education on an individual basis where evidence suggests it is needed.
- Staff receive regular input regarding strength of passwords including a strength-checking website and are made aware of the risks posed to the Academy's security through weak passwords.
- The Academy's network of devices are programmed to require hard-drives / USB sticks to be encrypted.

4. Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governor who oversees Child Protection and Safeguarding is Kym Jones.

All governors will:

- Ensure that they have read and understand this Policy.
- Agree and adhere to the terms on Acceptable Use Policies related to the school's ICT systems including the internet.

The Principal

The Principal is responsible for ensuring that this policy is presented to governors for approval when required and / or when appropriate following changes to the policy.

The Headteacher

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

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Designated Online Safety Lead / Strategic Lead for IT

Responsible for leading a team that ensures appropriate levels of security protection across the Academy including filtering, firewall and monitoring systems.

Responsible for ensuring this Policy reflects the Academy's approach to Online Safety and that it is updated as appropriate.

The Technical IT Team (Network Coordinators)

A weekly Online Safety (security) check is expected.

Checks ensure blocked access to:

- online gambling
- common social media sites
- Youtube (blocked for students only)
- pornographic content (using common search words)

Weekly checks are made against:

- the list of users that have accessed the Academy's wifi
- the password strength of *one staff user* and *one student user* at random

The Technical IT Team must ensure compliance regarding Online Safety training, including but not limited to:

- National Online Safety's 'Annual Certificate in Online Safety for ICT Leads'.
- NSPCC's CEOP-approved 'Keeping Children Safe Online' certification.

They are expected to make efforts to stay current regarding changes to technical solutions that impact Online Safety.

All staff

All staff who use the Academy's network and / or devices are responsible for adhering to the Staff Acceptable Use Policy relating to the Academy's ICT systems and the internet.

If working with pupils using devices and / or the network including the internet, they are also responsible for ensuring that pupils follow the relevant student Acceptable Use Policy.

All adults working within the Academy are responsible for responding appropriately to all reports and / or concerns about students' safety and wellbeing, both online and offline, and maintaining an attitude of 'it could happen here'.

Parents

Parents are welcome to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Familiarise themselves with their child's Acceptable Use Policy relating to use of the Academy's network, and the Academy's behaviour policy.

Clients and visitors

If appropriate, clients (e.g. organisations leasing the Academy's facilities) will be expected to agree to terms on Acceptable Use of the Academy's network.

5. Educating pupils about online safety

Pupils at Blue Coat CE Academy will be taught about online safety as part of the curriculum.

The Academy's PSHE Curriculum (2022-23) provides learning for all students in each year group on the following themes, **with specific content relating to Online Safety.**

Colour Coding related to the 4 Cs of recognised risk:

Content	**Contact**	**Conduct**	**Commerce**

Content – being exposed to illegal, inappropriate or harmful content.

Contact – being subjected to harmful online interaction with other users.

Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Note: there is naturally cross-over amongst the 4 Cs at times. Colour-coding reflects best-fit.

Key Stage 3

Theme	**Y7**	**Y8**	**Y9**
Health & Wellbeing	Managing risk and personal safety.	Self-conceptualisation: the impact of media and social media.	
	Healthy lifestyles: balance re. time spent online.		
Relationships	Forming, maintaining and managing positive relationships online.	Giving and withdrawing consent online.	Media portrayal of relationships.
	Online safety and support re. respectful relationships.		Grooming in the context of abuse, harassment and exploitation.
	Risks online.		Consent, the law and image-sharing.
Living in the Wider World	Culture – safer online behaviours.	Evaluating digital content.	Social media and influences.
	Online aspects of abusive behaviours.	Benefits of social media and engagement opportunities.	Privacy and risk online.
	Personal safety online when sharing information.		Financial decision-making and online exploitation.

Key Stage 4

Theme	**Y10**	**Y11**
Health & Wellbeing	Taking a balanced approach to time spent online and healthy lifestyle.	The effects of media on body image.
	Role models and influence.	Recognising adverse influences and risk of becoming involved in risky activity including cybercrime.
		The effects of advertising on health and cosmetic decision-making.
Relationships	Domestic abuse and sexual assault.	How the portrayal of sex through porn impacts relationships and expectations.
		Challenging hate crime.
	Developing the skills and readiness for sexual activity including online.	Sharing sexual images – ethical conduct online
		Unwanted attention and how to access support re. online harassment.

Living in the Wider World	Extremism online.	Data footprint and media information.
	Risky and emergency situations.	Job applications and CVs including online presence checks by potential employers.

Key Stage 5

Theme	**Y12**	**Y13**
Health & Wellbeing	.	
Relationships	Managing relationship boundaries online	Personal safety and consideration when in new relationships.
Living in the Wider World	Extremism and radicalisation.	The impact of online information and social media.
	Jobs and the workplace - cyber security and data protection.	

The safe use of social media and the internet will also be covered in other subjects where relevant.

Two whole-school Assemblies are delivered each academic year on the themes:

a) Online Safety including signposting to Student support links on the Academy's website and common report and block tools on social media.

b) Safer Internet Day covering the nationally shared theme.

Students across all Key Stages will be made aware of the Sharp System, an online tool (anonymous if students wish) for reporting concerns and abuse. A report made via the Sharp System triggers the Academy's Child Protection and Safeguarding systems. A link to this tool is available to students on the Academy's website.

6. Educating staff and governors about online safety

All staff are educated through:

a) The requirement to successfully complete the National Online Safety's 'Annual Certificate in Online Safety' best suited to their role (Teaching Staff / Support Staff / ICT Leads / SENCOs etc).

b) Regular cyber-attack simulations.

c) Regular communications regarding password strength.

d) Their Standard Level 1 Safeguarding training, completed annually or as part of induction procedures.

The Strategic Lead for IT and the Technical IT Team (Network Coordinators) are additionally certified in the NSPCC's CEOP-approved training, 'Keeping Children Safe Online'.

Governors are also annually expected to successfully complete the National Online Safety's 'Annual Certificate in Online Safety for Governors and Trustees'.

7. Educating parents and carers about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home where relevant.

Online safety may also be covered during parents' evenings and / or Open Evenings.

The Academy’s website will provide parents and carers with links to supportive tools including Thinkuknow and NSPCC help pages.

Where an Academy-networked device is made available on loan to a student, an NSPCC flyer on Online Safety is provided. The Academy’s filtering is in place on all Academy-owned devices.

Where a sixth form student in receipt of Bursary funding is provided with their own device, a conversation is held with parents / carers regarding Online Safety and it is made clear that the device is the property of the student and therefore filtering and settings cannot be the responsibility of the Academy.

If parents have any queries or concerns in relation to online safety, these can be raised with any member of staff who will be expected to then follow the Academy’s procedures around reporting Safeguarding concerns.

8. Cyber-bullying

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.

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 (upstanders as opposed to bystanders).

The PSHE curriculum detailed above will provide the backbone of the Academy’s education on cyber-bullying.

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

Where an incident of cyber-bullying occurs, the school will follow the processes set out in the Academy’s behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

Authorised members of staff can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

1. Poses a risk to staff or pupils, and/or
2. Is identified in the school rules as a banned item for which a search can be carried out, and/or
3. Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

1. Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.
2. Explain to the student(s) why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
3. Seek the student(s) cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

1. Cause harm, and/or
2. Undermine the safe environment of the school or disrupt teaching, and/or
3. Commit an offence

If inappropriate material is found on the device, it is up to the DSL, Headteacher or Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

1. They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
2. The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

1. **Not** view the image

2. Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE’s latest guidance.

Any searching of pupils will be carried out in line with the DfE’s latest guidance and wider policies.

9. Acceptable use of the internet in school

All users of the school’s network including pupils, staff and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet.

Sixth form students may access wifi for independent study purposes, reflected in the Acceptable Use Policy for KS5 students. They may use mobile phones and / or other personal devices in study spaces such as the LRC, Click and Common Room. Security is ensured using a pass system which gives KS5 users (who have agreed to the relevant Acceptable Use Policy) credentials that allow one known device to access the internet onsite. This ensures online activity by students using the Academy’s wifi can be appropriately monitored.

Staff may access the Academy’s wifi using “Staff BYOD” access which recognises their user credentials on their device.

External clients (for example organisations leasing the Academy’s facilities) will be expected to read and agree to the school’s terms on acceptable use if relevant to their use of the Academy’s estate.

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. It must not contravene the Academy’s Policies on students’ behaviour and staff conduct.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school.

However, students in **Key Stages 3 and 4 are not permitted to use them** during the school day.

This includes during:

3. Lessons
4. Form time
5. Clubs before or after school, or during any other activities organised by the school

Key Stage 5 students (sixth formers) are allowed to use their personal devices for study purposes during their independent study time. Appropriate locations include the LRC, Click and Sixth Form Common Room. The Academy has devised a system for enabling sixth form students to access the Academy's wifi for this purpose. The terms and conditions within the Academy's Key Stage 5 Acceptable Use Policy apply at all times.

11. Staff using work devices outside school

All staff members must take appropriate steps to ensure their devices remain secure.

The Academy's Acceptable Use Policy for staff and governors contains detail.

This includes, but is not limited to:

a) Keeping devices used for work purposes and Academy data 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)

b) Ensuring hard-drives, if staff are choosing to take the risk of using them, are encrypted. The Academy's network of devices are programmed to require hard-drives / USB sticks to be encrypted.

c) Ensuring use of any shared home devices does not compromise the security of the Academy's data.

Staff may access the Academy's wifi using "Staff BYOD" access which recognises their user credentials on their device.

All staff have Microsoft A3 licensing as a minimum to ensure appropriate levels of security protection to mitigate against the risks of cyber attacks. A select group of staff have Microsoft A5 licensing representing the highest level of protection to reflect their access to sensitive data and / or finance.

All staff have MFA (Multi Factor Authentication) enabled on their Microsoft Office accounts. For the majority of staff, this is enabled offsite only to minimise disruption to their roles onsite. Mirroring the approach to licensing, a select group of staff have MFA enabled both on and offsite. This reflects their access to sensitive data and / or finance.

The Academy has eliminated the use of Remote Access technology, reducing security risks through the use of cloud file storage and MIS hosted in the cloud. The link to access the MIS remotely is only made available within the Academy's native Office365 environment.

The Strategic Lead for IT and their team conduct regular simulations of cyber attacks using Microsoft security tools. The intention is to harden colleagues' security stance on malicious links and credential harvesting, and to provide further education on an individual basis where evidence suggests it is needed.

Staff receive regular input regarding strength of passwords including a strength-checking website.

Members of the Senior Leadership Team and colleagues whose roles see them work remotely on data are provided with a networked device. These members of staff are expected to use this device in preference to any other personal device when carrying out their role in order to protect themselves, their work and our data within the security of the Academy's network.

Staff members must not use any device in any way which would violate the school's terms of acceptable use, or damage the reputation of staff, students or the Academy.

If staff have any concerns over the security of their device, they must seek advice from the Technical IT Team (Network Coordinators and / or the Strategic Lead for IT).

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT acceptable use. 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 using staff disciplinary procedures and the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Strategic Lead for IT. At every review, the policy will be shared with the governing board.

14. Links with other policies and resources

This Online Safety Policy makes reference and / or is related to the following:

- DfE guidance on Keeping Children Safe in Education
- Child protection and safeguarding policy
- ICT and internet acceptable use policies
- The PSHE Curriculum
- Flyer: NSPCC's Top Tips on Online Safety (parents and carers)
- The National Online Safety 'Annual Certificates'
- The NSPCC's CEOP-approved 'Keeping Children Safe Online' certification.
- Latest DfE guidance on searches.
- The Sharp System for (optionally anonymous) reporting by students
- The reporting tool 'CPOMS'
- The device management and monitoring tool 'Senso'.
- The student behaviour policy
- Staff disciplinary procedures
- The Staff Code of Conduct