Orchard Hill College Academy Trust

ST PHILIP'S SCHOOL
ONLINE SAFETY POLICY

Written by:	Wendy Clements
Reviewed by:	Debbie Battle
Date of last review:	January 2023
Date of next review:	January 2024

Online safety policy

Introduction

At St Philip's School, the safety and welfare of our pupils/students is of the utmost importance. Ensuring that pupils/students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

This policy sets out our approach to online safety, whether using new technology within St Philip's School or at home, including accessing remote learning.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils/students, 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 (herein referred to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- 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;
- 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
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Statutory requirements

This policy is based on the Department for Education's (DfE's) 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
- 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.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities

Governors will:

- Review and approve this policy not less than annually.
- Agree and adhere to the IT Acceptable Use Policy.
- Ensure that online safety is a running and interrelated theme of St Philip's School's whole school approach to safeguarding and related policies and/or procedures, including the school's Safeguarding and Wellbeing Offer.
- Ensure that the school's approach to promoting and upholding online safety is suitably tailored to the needs and aspirations of St Philip's School pupils/students as well as the specific risks and opportunities they may encounter as a result of their needs and within their local communities.

The Principal will:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout the school.
- Review and update this policy not less than annually.
- Monitor the impact of online safety measures as set out in this policy, through regular monitoring of safeguarding practice across the school (e.g. termly safeguarding audit, data analysis, review of Safeguarding and Wellbeing Offer, pupil/student voice).
- Ensure that staff have access to high quality and relevant training on online safety matters, to enable them to effectively support pupils/students.

The Designated Safeguarding Lead (DSL) will:

- Take lead responsibility for online safety in school.
- Support the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Work with the Principal, ICT manager and other staff as necessary to address any online safety issues or incidents.
- Manage all online safety issues and incidents in line with the Child Protection Adult Protection & Safeguarding Policy.
- Ensure that any online safety incidents are logged via SIMS, reported to the DSL/Deputy DSL and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Liaise with other agencies and/or external services as necessary.
- Provide regular reports on online safety in school to the Principal.

OHCAT IT staff will:

- Put 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/students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduct full security checks and monitoring of the school's ICT systems on a regular basis
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files.

All staff, including contractors, agency staff and volunteers will:

- Maintain an understanding of this policy
- Implement this policy consistently
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet, and ensure that pupils/students follow the school's terms on acceptable use
- Work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Respond appropriately to all safeguarding reports and concerns, including those relating to cyber-bullying and sexual violence/harassment (whether on- or offline), maintaining an attitude of 'it could happen here'

Parents/carers are expected to:

- Notify a member of staff or the Principal 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.

Parents/carers 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

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. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils/students about online safety

Online safety is revisited annually through IT and PSHE lessons. It is delivered through a rolling programme which builds on information from the previous years. All activities are adapted and differentiated to meet the needs of the students in the group. In addition, individual or tailored group sessions are delivered to students, or groups of students, who require support to address a specific online safety risk.

Communication with families

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be discussed, when necessary, during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

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

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. As with 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. Please also refer to our Anti-Bullying Policy, Behaviour Policy and the Child Protection, Adult Protection & Safeguarding Policy.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils/students understand what it is and what to do if they become aware of it happening to them or others, including becoming aware that they have participated in cyber-bullying. We will ensure that pupils/students 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/students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Opportunities to discuss include during form time, within the curriculum e.g. PSHE, during assemblies and Student Council meetings.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Behaviour Policy, including safeguarding and support pupils/students involved. Where illegal, inappropriate or harmful material has been spread among pupils/students, the school will take all necessary steps to safeguard pupils/students including using all

reasonable endeavours to ensure the incident is contained and liaising with police or other external agencies as appropriate.

Examining electronic devices

The Principal, and any member of staff authorised to do so by the Principal, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils/students and staff
- Explain to the pupil/student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil/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:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Principal in conjunction with the Senior Leadership Team/DSL 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:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil/student 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 Youth-Produced imagery), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL immediately. The DSL will decide on what to do next, in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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

Acceptable use of the internet in school

All staff, governors, volunteers and other members of the St Philip's School community are expected to adhere to the IT Acceptable Use Policy. Parents are expected to discuss the Acceptable Use Policy to their son/daughter and sign the acceptable use 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.

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

Use of mobile devices in school

Pupils/students may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school *except during own device club on Friday afternoon.*

Students are expected to hand their mobile phone in to the school office through using their form group's phone box, or to leave their phone with a trusted member of staff.

Any use of mobile devices in school by pupils/students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil/student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Rules for publishing material online (including images of pupils/students)

School websites are a valuable tool for sharing information and promoting pupils' and students' achievements. We recognise the potential for abuse. Therefore the following principles will always be considered:

- If an image, video or audio recording of a pupil/student is used, their surname should not be used (including in credits).
- Staff **must not** take photographs of pupils or students using their personal devices – all pupil/student photographs must be taken using OHCAT equipment and transmitted through OHCAT systems.
- Files should be appropriately named in accordance with these principles.
- Only images of pupils/students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Parents/carers are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respectful.
- Material should be checked by a member of the school's Senior Leadership Team before being published.
- Staff must not post or transmit images of pupils/students or families via their personal social media accounts. St Philip's School considers social media to be any technology-based platform used for interacting or discussion via voice, text, video or pictures. Please refer to the Social Media Policy for further information.
- Staff should not post any images of staff on any social media without first obtaining permission from those person(s) in the image.

Children and young people use a variety of online tools for educational purposes. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and will be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photos and videos of school events are permitted to be taken by parents and carers, they will be asked not to publish them on any public area of the Internet, including social networking sites.

Training

All new staff members 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 receive refresher training at least once each academic year as part of safeguarding training. Staff also receive regular updates about how to protect and conduct themselves professionally online and to ensure that they have an awareness of

issues surrounding modern technologies, including safeguarding. Updates are delivered through CPD, staff meetings and email updates which also signposts to relevant external resources and sources of support.

By way of this training, all staff are 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.
- Children and young people with SEND may be especially vulnerable to online abuse.
- It is incumbent on all staff to maintain professional relationships with pupils/students and families at all times, including within the digital world.

Training also supports staff to:

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

The DSL and deputy DSLs undertake Level 3 child protection and safeguarding training, including online safety, yearly.

Governors receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers receive appropriate training and updates, if applicable.

Please refer to the Child Protection, Adult Protection & Safeguarding Policy for further information.

Guidance on the use of social media

We recognise that many staff will actively use social media platforms for a variety of reasons, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to pupils/students or colleagues via social media networks; discretion and professional conduct is essential. Posts that bring St Philip's School or OHCAT into disrepute and/or breach confidentiality

are likely to result in disciplinary action. Staff must review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child or young person in any OHCAT provision or from ex-pupils/students who are still minors. This is to avoid any possible misinterpretation of motive or behaviour which could be construed as grooming.

Staff must not give their personal contact details to pupils/students, including e-mail, home or mobile telephone numbers. All correspondence must be via OHCAT systems.

Please refer to the Social Media Policy, the Staff Code of Conduct and the IT Acceptable Use Policy for further details.

Monitoring arrangements

This policy will be reviewed and approved annually by the Principal and the Local Governing Body.

Related policies and documentation

Anti-Bullying Policy
Anti-Radicalisation Policy
Child Protection, Adult Protection and Safeguarding Policy and Procedures
Data Protection Policy and related documentation
Dignity at Work Policy
IT Acceptable Use Policy
Safeguarding & Wellbeing Offer
Positive Behaviour Policy
Social Media Policy
Staff Code of Conduct
Student Mental Wealth, Health and Wellbeing Policy
Management SG flow chart 2022-23