University of Brighton Academies Trust

WEST ST LEONARDS PRIMARY ACADEMY

POLICY

Policy title	Online Safety
Adapted by	Director of Governance and Admissions/Safeguarding and Welfare Lead/IT Director
Policy owner	Deputy CEO: School Improvement

Status	Approved
Summary of change	Annual update to reflect Keeping Children Safe in Education Sept 2023

Approval date	15 September 2023
Approval authority	Board of Trustees – Education and Standards Committee Chair
Review date	1 September 2024

Each academy in The University of Brighton Academies Trust has an Online Safety policy to support the Trust-wide safeguarding culture.

Role	Name	Contact details
Designated Safeguarding Lead (DSL)	Angela Scott	01424 422 080
Deputy Designated Safeguarding Lead	Tom Elvy	01424 422 080
Deputy Designated Safeguarding Lead	Serena Oberheim	01424 422 080
Nominated Trustee for safeguarding and child protection	Siobhan Denning	s.denning@brightonacademiestrust.org.uk

1. Policy Aims

- This online safety policy has been adapted by West St Leonards Primary Academy (the academy), involving staff, pupils/students and parents/carers, Trustees and local governors, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education 2023, Early Years and Foundation Stage and the Sussex Child Protection and Safeguarding Partnership procedures. (Click here)

- The purpose of this online safety policy is to:
  - Safeguard and protect all members of the academy community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- The academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
  - **Commerce/contract:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams and sextortion (online sexual coercion and extortion of children).

2. Policy Scope

- The academy believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils/students and staff are protected from potential harm online.
- The academy identifies that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- The academy believes that pupils/students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

- This policy applies to all staff including the Board of Trustees, Local Governing Body (LGB) members, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the academy (collectively referred to as "staff" in this policy) as well as pupils/students, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices[1], or where pupils/students, staff or other individuals have been provided with Trust/academy issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to member of the school/academy. The Behaviour in Schools guidance (2022) further reinforces this stating: *Maintained schools and academies' behaviour policies should set out what the school will do in response to non-criminal poor behaviour and bullying which occurs off the school premises or online and which is witnessed by a staff member or reported to the school.*
- In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school. Action can only be taken over issues covered by the published Behaviour Policy

2.1 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Academy Preventing Bullying policy
- Acceptable Use Policies (AUP)
- Staff Code of conduct
- Behaviour and discipline policy
- Academy Child protection and safeguarding policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection
- Photography and image sharing policy
- Social media policies

2.2 Online safety in community activities, after-school clubs and tuition

- When our school hires out or lets school facilities/premises to organisations or individuals (e.g. community groups, sports associations and service provider to run community or extra-curricular activities), we ensure that appropriate arrangements are in place to keep children safe.
- We seek assurances that where services or activities are provided separately by another body (not under direct supervision or management of our school staff) there are appropriate safeguarding and child protection policies and procedures in place (including online safety) and will inspect these as necessary. This applies regardless of whether or not the children who are attending these services are on our school roll.
- Safeguarding arrangements are clearly detailed in any transfer of control agreement (i.e. lease or hire agreement).

[1] Filtering is not applied to personally owned devices (unless requested). Where filtering is applied to personally assigned devices such as DFE devices, filtering is configured however active monitoring and reporting is not available.

- The DfE has published Keeping Children Safe during community activities, after-school clubs and tuition for organisations and individuals who provide these activities for children and young people and this document contains a section on online safety which makes clear that the provider should have an online safety policy or acceptable use policies in place as well as appropriate filtering and monitoring. A staff behaviour policy should also include information on relationships and communications between children (and parents) and staff/volunteers, including the use of social media.

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; this policy will be reviewed at least annually
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate.
- The Safeguarding Link Trustee will report on, at least, an annual basis to the Board of Trustees on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) has lead responsibility for online safety.
    - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- The digital and technology standards in schools guidance states that the governing body should identify and assign a member of the leadership team and a governor to be responsible for ensuring the standards relating to filtering and monitoring are met. The governor responsible for this is the Safeguarding Link Trustee.
- The academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Board of Trustees will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running interrelated theme in appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policies, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place which enable technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).

4.2 The Principal will:

- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement
- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the academy's IT system through the suitable and appropriate filtering and monitoring systems in place. They will have an awareness and understanding of the provisions in place and will work with technical staff to monitor the safety and security of our systems and networks, ensuring that these are regularly reviewed for effectiveness.
- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.
- Ensure that they regularly review the effectiveness of filters and monitoring systems; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- In conjunction with the ICT Team, ensure that the DfE's filtering and monitoring standards for schools and colleges are being met.
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all pupils/students to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Recognise that a one size fits all approach may not be appropriate for all children and a more personalised or contextualised approach to online safety is used for more vulnerable children and children with SEND
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school or college safeguarding approach and know how to escalate concerns when identified.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.
- Audit and evaluate online safety practice, ideally annually, to identify strengths and areas for improvement.
- Communicate with parents regarding the importance of children being safe online, the systems being used in the academy and information regarding what their children are being asked to do online by the academy.

4.3 The Designated Safeguarding Lead (DSL) will:

- Be an appropriate senior member of staff from the academy leadership team
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.

- Liaise with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring, and have the relevant knowledge and up to date training required to keep pupils/students safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils/students with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the academy's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns as appropriate.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input, including from pupils.
- Provide information to the Principal to ensure that online safety concerns are reported to the LGB via the Principal's report – the LGB will report unresolved concerns to the Board of Trustees via their regular report.

4.4 It is the responsibility of the School Improvement Team to:

- Monitor and evaluate incidents of online/cyber bullying, including sexualized incidents, on a termly basis, providing challenge and support as necessary

4.5 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of academy systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the academy's safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and consistently implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reinforce the school's online safety messages when teaching lessons online

4.6 It is the responsibility of pupils/students (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities provided by the academy.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Understand the importance of good online safety practice out of school, and understand that this policy covers their actions outside of school if related to their membership of the academy
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, or other support services, if there is a concern online, and support others that may be experiencing online safety issues.

4.7 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement *and* acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the academy, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4.8 The Trust ICT team will:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures and compliance with DfE'S filtering and monitoring standards for schools and colleges.
- Implement appropriate security measures to ensure that the academy's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils/students

- The academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst pupils/students by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils/students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. This should include the use of generative AI tools and services.
  - Teaching pupils/students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The academy will support pupils/students to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying age-appropriate acceptable use posters in all rooms with internet access.
  - Informing pupils/students that network and internet use will be monitored for safety and security purposes and in accordance with legislation. This should include information about whether school-owned devices are also monitored when not connected to the academy network.
  - Rewarding positive use of technology in line with positive reinforcement and rewards outlined in the academy's behaviour policy.
  - Implementing appropriate peer education approaches.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking pupil/student voice when writing and developing online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Pupils/students

- The academy recognises that some pupils/students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- The academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils/students. In regards to a pupil with a physical disability, hardware amendments would be made in line with NHS guidance. Software use, such as the use of Sono Flex for children requiring additional support in communication, will also be implemented. Life skills lessons also includes keeping safe online.
- When implementing an appropriate online safety policy and curriculum the academy will seek input from specialist staff as appropriate, including the SENCO, Looked After Children Designated Teacher as well as the Facility's specialist teacher.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff, Trustees and local governors, as part of induction.
- Ensure that all staff members, Trustees and local governors, complete "Cyber Security Training for School Staff" course provided by the National Cyber Security Centre
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - This will be achieved through inclusion in safeguarding training.
    - This will cover the potential risks posed to pupils/students (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the academy, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils/students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils/students, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- The academy recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
        - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.
    - Providing them with information about our approach to filtering and monitoring as well as information about the types of things that children will be doing online.

6. Reducing Online Risks

- The academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments including a Data Protection Impact Assessment before use in the academy is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

7. Safer Use of Technology

7.1 Classroom Use

- The academy uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
    - Bespoke hardware and software for children with a physical disability, implemented under the guidance of medical professionals.
- All academy owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
    - Each member of staff and pupils from Year 3 to Year 6, have individualised logins that must remain the property and responsibility of the individual- no sharing is permitted. The academy has also

implemented a 'safe search' weekly monitoring report where any searches deemed malicious or inappropriate are recorded and a notification is sent to the Principal of the academy.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The academy will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
    - Whilst the firewall does work to block unsafe searches and search engines of questionable origin, the school continues to promote the use of Google as a known safe search engine. Setting around the use of Google Safesearch remain under the control of the central Trust ICT team, as do the settings for any firewall controlling internet traffic.
- We will ensure that the use of internet-derived materials, by staff and pupils/students complies with copyright law and acknowledge the source of information.
- Supervision of pupils/students will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils/students age and ability.
    - **Key Stage 2**
        - Pupils/students will use age-appropriate search engines and online tools.
        - Pupils/students will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, pupils/students and visitors will read an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

- The academy is compliant with the DfE's filtering and monitoring standards for schools and colleges. This is checked and reviewed at least annually.

7.3.1 Decision Making

- The University of Brighton Academies Trust have ensured that our academy has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The Trust is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- The decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances and is reviewed at least annually by the Director of IT with input from the Trust Safeguarding and Welfare Lead; the outcome of this review is reported to the Safeguarding Trustee and included in the annual safeguarding report to the Board of Trustees. A review will also be carried out following the identification of a safeguarding risk or any changes in working practice or if new technology is introduced. We follow the guidance outlined in the DfE filtering and monitoring standards when carrying out the review.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The Designated Safeguarding Lead will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate using the Safer Internet Centre guidance on appropriate filtering and appropriate monitoring.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils/students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- We use industry standard web filters which will block sites that are categorised as: pornography, racial hatred, extremism, and other sites of an illegal nature.
- Our filtering provider is a member of the Internet Watch Foundation (IWF).
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The filtering system blocks all sites on the Counter Terrorism Internet Referral Unit (CTIRU) list.
- The Trust ICT Team works with academies and central teams to ensure that our filtering lists are continually reviewed.
- If pupils/student or staff member discover unsuitable sites, they will be required to:
    - Close the website – if unable to do so then switch off the monitor/screen.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and central ICT team via remotesupport@brightonacademiestrust.org.uk
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.

7.3.3 Monitoring

- We will appropriately monitor internet use on all academy owned or provided internet enabled devices and personal devices which connect to the Trust network. This is achieved by:
    - Monitoring of children by teaching staff when laptops and tablets are being used.
    - Use of reporting capabilities of the school's firewall systems to receive weekly reports around potential unsafe searches which are then promptly investigated.
    - Operational DSL to promptly investigate any allegation highlighted in the classroom.
    - Use methods of communication amongst academy staff where the chronology can be reviewed in the event of concerns raised.
    - Centralised monitoring and alert systems administered by the Trust ICT Team.
- If a concern is identified via monitoring we will respond in line with the academy Child Protection and Safeguarding policy
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Data Protection policy on the Trust website

7.5 Security and Management of Information Systems

- We adhere to and meet the DfE cybersecurity standards. Further information is available in the DfE cybersecurity standards https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges
- We take appropriate steps to ensure the security of our information systems, including:
    - Protecting all devices on every network with a properly configured boundary or software firewall
    - Keeping an up-to-date list of every device that is able to access the network and ensuring their security features are enabled, correctly configured and up to date
    - Ensuring that accounts only have the access that they require to perform their role and should be authenticated to access data and services
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on our network,
    - The appropriate use of user logins and passwords to access our network.
        - Specific user logins and passwords will be enforced for all[2]
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found in Acceptable Use policies.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year *3*, all pupils/students are provided with their own unique username and private passwords to access our systems; pupils/students are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system – these are a minimum of 10 characters and in line with Microsoft security recommendations
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.
    - Use two-factor/two-step verification for all accounts which have access to personal or sensitive operational data and functions

[2] this should be in place for all except Early Years and Foundation Stage children and some pupils/students with SEND

7.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our academy address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Photography and image sharing policy, Data Protection policy, Acceptable Use policies, Staff Code of Conduct, Academy Behaviour and Preventing Bullying policies and Social Media policy.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including Acceptable Use policies and the Code of Conduct and academy behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- Members of the community will immediately inform the safeguarding officer if they receive offensive communication, and this will be recorded in our safeguarding files/records.

7.8.1 Staff email

- The use of personal email addresses by staff for any official academy business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils/students and parents.

7.8.2 Pupil/student email

- Pupils/students will use provided email accounts for educational purposes.
- Pupils/students will read an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the academy.

7.9 Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function and it is this type of platform that will be used in the academy.

- When planning the use of live stream platforms within remote learning our academy will:
    - Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
    - Ensure that staff are trained to use the technology.
    - Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
    - Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

Protocols for the use of live streaming are included in the Trust Acceptable Use policies for students/pupils and staff.

7.10 Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, the content will be monitored by a member of staff along with the interactions/behaviour of the learners taking part.
- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and, then, monitor some sessions to check they are in accordance with the policy.
- We are aware that our filtering and monitoring systems may not necessarily prevent inappropriate content from being shared in a live-streamed event as this is happening in real-time.

7.11 Using video calls for 1:1 sessions with children

- The academy may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT and parental consent given.
- Where the communication with an individual child does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
- In either case both adults will be present before the child is admitted to the online session.

7.12 Management of Applications (apps) used to Record Children's Progress

- We use SIMs, Target Tracker/SONAR, Smartgrade and other on line assessment systems to track pupils/students progress.
- The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store pupils/students' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils/students' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

Detailed information regarding the use of Social Media can be found in Acceptable Use policies, Staff Code of Conduct and the Social Media policy

9. Use of Personal Devices and Mobile Phones

- The academy recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the academy.

9.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of the academy community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of the academy community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used at times where the focus is to be on the children. The environments where this occurs are also environments where mobile phones and personal devices are not to be used; this includes specific areas within the site such as changing rooms, toilets and when staff take pupils to swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

- All members of the academy community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.
- Further information on the use of personal devices is available in Acceptable Use policies, the Academy behaviour policy and the Staff Code of Conduct.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils/students or parents/ carers is required.
- Academy mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Academy mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including, but not limited to, breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content. Detailed information can be found in the Academy Child Protection and safeguarding policy and procedure.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Child-on-child online sexual violence and sexual harassment

- Our academy has accessed and understood part 5 of Keeping Children Safe in Education September 2023.
- The academy recognises that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and preventing bullying policy.
- The academy recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The academy also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational academy, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Sussex Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')

- The academy recognises youth produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people,.
- The academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods. This is also supported by visits by the police to have them explain the dangers of social media to pupils at the academy and how they can report this malicious communication.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using academy provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is
    - a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.– **in most cases, images or videos should not be viewed. The UKCIS/DSIT guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people provides information on the steps to be taken if an image does need to be viewed.**
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant East or West Sussex Safeguarding Child Partnership's procedures.
    - Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Children's Social Care and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support. This will include signposting to services such as *report remove* and *take it down*
    - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance.
        - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- The academy will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The academy recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that a link to CEOP is visible and available to learners and other members of our community on the online safety page of the academy website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant East or West Sussex Safeguarding Child Partnership's procedures.

- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using academy provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns to CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Standards and Learning Effectiveness Service, Safeguarding in Education team and/or Police.
- If learners at other academies are believed to have been targeted, the DSL (or deputy) will contact the Police.

11.4 Indecent Images of Children (IIOC)

- The academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service or Safeguarding in Education team.

- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant East or West Sussex Safeguarding Child Partnership's procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy DSL) is informed, who will investigate the incident.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the academy provided devices, we will:
  - Ensure that the DSL (or deputy DSL) and Principal are informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted once directed by police.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on academy provided devices, we will:
  - Ensure that the Principal is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- All staff at the academy understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated here.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which is in the academy's behaviour policy on the website.

11.6 Cybercrime

- The academy will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

11.7 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at the academy and will be responded to in line with existing policies, including anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service, Safeguarding in Education team and/or Sussex Police.

11.8 Online Radicalisation and Extremism

- The academy will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff, Trustee or local governor may be at risk of radicalisation online, the Principal will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links

Pan-Sussex Safeguarding Children Partnership

- www.sussexchildprotection.procedures.org.uk/

Sussex Police:
www.sussex.police.uk

For non-urgent Police contact 101 or 01273 470101

If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for schools

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

There is a wealth of information available to support schools and parents/carers to keep children safe online. See Keeping Children Safe in Education 2023 (Annex B) for more resources.