Title	Online Safety
Associated Policies	• Acceptable Use Policy (GU.06) • Safeguarding and Child Protection (TPO/HS/05) • Professional and Safe Conduct (TPO/STA/10) • Whistleblowing (TPO/STA/19) • Anti-Bullying (TPO/STU/01) • Data Protection (TPO/STA/25) • Behaviour and Discipline (TPO/STU/03)

REVIEWED: September 2023

NEXT REVIEW: September 2024

Or as required in response to developments

Contents

Document Control 2
Summary of Changes 2
Policy Statement 3
Legislation and Guidance 4
How should this policy be applied? 4
Who is responsible for carrying out this policy? 5
What are the principles behind this policy? 5
Who is responsible for online safety and what are their responsibilities? 6
Procedures 11
Educating students about online safety - curriculum 13
Educating parents and carers about online safety 15
Use of mobile phones and smart technology 15
Examining Electronic Devices 16
Policy Review 17
Appendix A – Cyber Crime 18
Appendix B – Relevant Legislation 19
Appendix C - Online Safety guidance and resources 23

Document Control

Date of last review:	September 2023	**Author:**	Head of Safeguarding
Date of next review:	September 2024	**Version:**	5
Approved by:	Strategic Delivery Group	**Status:**	Draft

Summary of Changes

- Updated references to Keeping Children Safe in Education (2023) throughout the policy.
- Updated policy aims, to include clarifying the roles and responsibilities in relation to online safety, including filtering and monitoring ***(paragraph1.3)***.
- Added *Meeting Digital and Technology Standards in Schools and Colleges* and *Education for a Connected World* to relevant legislation and guidance ***(paragraph 2.1).***
- Clarified that the scope of the policy extends to the use of cameras and all other internet enabled devices when used on the school site ***(paragraph 3.4)***
- Clarified that the Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection (including online safety) ***(paragraph 4.1)***
- Added self-generated artificial intelligence (AI) to the list of possible online safety incidents ***(paragraph 5.3)***
- Updated the responsibilities of all staff in relation to Online Safety ***(paragraph 6.1)***
- Updated the responsibilities of the Executive Leadership Team ***(paragraph 6.2)***
- Added the responsibilities of the Head of Safeguarding ***(paragraph 6.3)***
- Updated the responsibilities of the Principal ***(paragraph 6.4)***
- Updated the responsibilities of Governors ***(paragraph 6.5)***
- Added the responsibilities of Trustees ***(paragraph 6.6)***
- Updated the responsibilities of the DSL, including clarifying the responsibilities that should be discharged via the Online Safety Group ***(paragraph 6.7)***
- Updated the responsibilities of staff and contractors managing the technical environment, to include reference to the DfE Cyber Security and Filtering and Monitoring Standards ***(paragraph 6.8)***
- Updated the responsibilities of PSHE/RSHE Leads ***(paragraph 6.9)***
- Clarified the actions that will be taken by each academy in relation to filtering and monitoring ***(paragraph 7.2.1)***
- Clarified expectations in relation to the use of email, including reference to the communications charter and the impact of email on staff workload ***(paragraph 7.7.4)***
- Clarified expectations in relation to staff use of mobile phones and smart technology ***(paragraph 10.3)***
- Updated content and links within Appendix A relating to Cyber Crime

1. Policy Statement

1.1 Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory and non-statutory guidance. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing. it is designed to sit alongside the Trust's statutory Safeguarding and Child Protection Policy.

1.2 Any safeguarding related issues and concerns will be dealt with in line with the Safeguarding and Child Protection Policy. This may involve making referrals to Children Social Care or Police, where appropriate.

1.3 Brooke Weston Trust is committed to promoting the welfare and safety of our students when using digital technologies. The Trust recognises the importance of the contribution it can make to protecting and supporting students across its Academies in their use of these technologies.

1.4 This policy aims to:

- Set out expectations for the online behaviour, attitudes and activities and use of digital technology (including when devices are offline) for all members of the BWT community.
- Help safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g., for filtering and monitoring), curriculum leads (e.g., RSHE) and beyond.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - For the protection and benefit of the children and young people in their care.
    - For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as the Behaviour and Discipline Policy or Anti-Bullying Policy).
- Incorporate all aspects of child protection and safeguarding that may be affected by digital technology as well as Brooke Weston Trust's use of technology with its Academies.
- Highlight the importance of online safety as a safeguarding issue.
- Clarify roles and responsibilities in relation to online safety, including filtering and monitoring.

1.5 The Trust aims to have robust processes in place to ensure the online safety of students, staff, volunteers and governors. This will be achieved by establishing clear mechanisms to identify, intervene and escalate an incident where appropriate.

1.6 An effective approach to online safety empowers us to protect and educate each academy community in its use of technology.

1.7 The Trust will refer to the most recent government, DfE and ICO guidance and documentation with regard to Data Protection, data storage and privacy compliance.

2. Legislation and Guidance

2.1 This policy is based on the Department for Education's statutory Safeguarding Guidance, Keeping Children Safe in Education and its advice for schools on:

- Meeting digital and technology standards in schools and colleges (2023)
- Teaching Online Safety in Schools (DfE, 2019)
- Preventing and Tackling Bullying (DfE, 2017)
- Relationships and Sex Education (DfE, 2019)
- Behaviour in Schools (DfE, 2022)
- Searching, Screening and Confiscation (DfE, 2022)
- Protecting Children from Radicalisation (DfE, 2015)
- Education for a Connected World (UKCIS, 2020)
- Sharing nudes and semi-nudes: Advice for education settings working with children and young people responding to incidents and safeguarding children and young people (UKCCIS, 2020)

2.2 Further legislation and guidance is detailed in Appendix B.

3. How should this policy be applied?

3.1 This policy applies to all members of the Trust community, incorporating students, staff (including teaching, supply and support staff), governors, volunteers, contractors, parents, visitors and community users.

3.2 This policy applies to any individual who is given access to BWT's digital technology, networks and systems, whether on-site or remotely, and at any time, or who uses technology in their professional role within the Trust. The policy also extends to any member of the BWT community accessing the internet via personal devices, including smart devices, and via 3G, 4G or 5G.

3.3 BWT expects all Academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the internet, both on and off the school site. This will include imposing rewards and sanctions for behaviour. The 'In Loco Parentis' duty allows the academy to report and act on instances of online bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material, including reporting to the police, social media websites, and hosting providers on behalf of pupils.

3.4 The Online Safety policy covers:

- The online safety curriculum intent, delivery and impact.
- School based IT systems.
- School based intranet and networking.
- School related external internet, including but not exclusively, extranet, e-learning platforms, blogs, and social media websites.
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing.
- School IT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets.
- Student and staff personal IT equipment when used in school and which makes use of school networking, file-servers or internet facilities.
- Tablets, mobile phones, laptops and other camera- and/or internet enabled devices when used on the school site.

4. Who is responsible for carrying out this policy?

4.1 Whilst all staff have a responsibility for ensuring the online safety of all members of the academy community, the Designated Safeguarding Lead takes lead responsibility for safeguarding and child protection (including online safety).

4.2 Principals should ensure that all academy staff and governors are aware of the Online Safety policy and procedures and of their responsibilities under it. It is the responsibility of the Principal to ensure that breaches of the policy are investigated and addressed.

4.3 Staff and governors are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the academy or Trust into disrepute or damage their own professional reputation.

4.4 The implementation of this policy will be monitored by the academy's Senior Leadership Team, governors and Trust Leadership Team and remain under review by the Brooke Weston Trust Safeguarding Review Group.

4.5 All staff, students, parents and carers have responsibilities as outlined in this policy. Online safety is everyone's responsibility.

5. What are the principles behind this policy?

5.1 Online safety risks are traditionally categorised as one of the **4 Cs: Content, Contact, Conduct** or **Commerce.** These areas remain a helpful way to understand the risks and potential response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four.

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and /or pornography, sharing other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff, pupils or students feel at risk, please report it to the Anti-Phishing Working Group apwg.org

5.2 The most likely areas of risk to students are:

- Exposure to illegal inappropriate or harmful material.
- Subject to harmful online interactions with other users.
- The individuals' personal online risky behaviour that then leads to harm.

This is not exhaustive.

5.3 The definition of an online incident is:

"*Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the academy and/or BWT. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means*".

Examples of issues that may be part of an incident include:

- Self-generative artificial intelligence (AI)
- Self-generated sexual imagery (also known as nude or semi-nude imagery)
- Child on child abuse – online bullying
- Sexual abuse – 'grooming'
- Upskirting
- Online sexual harassment
- Child Criminal Exploitation/Child Sexual Exploitation
- County Lines
- Radicalisation – extremism, radicalisation and terrorism
- Homophobic/transgender/racist/faith based/offensive language or behaviour
- Misogyny/misandry
- Breaches of filtering
- Exposure to illegal, inappropriate or harmful content
- Cybercrime (see Appendix A)

The above list is not exhaustive, and all incidents will be responded to in line with the relevant policies, including Anti-Bullying, Behaviour and Discipline, Dealing With Allegations Against Staff and the Safeguarding and Child Protection Policy. DSLs will also follow procedures contained within the BWT CPOMS Toolkit when responding to incidents of harmful sexual behaviour, including nude and semi-nude images.

5.4 The Trust has a responsibility for ensuring that resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

5.5 The Trust seeks to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in their academy and in their future in their chosen careers and workplaces.

5.6 Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and will be continually reinforced and monitored as students' progress through their school life.

5.7 Academy's will use their reasonable endeavours to ensure that procedures, rules and safeguards are in place for remote learning.

5.8 The Trust actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students and staff, and to protect the reputation of the individual academies and the Trust. The Trust seeks to promote a cyber-awareness culture that ensures all staff, students and governors engage with ongoing opportunities to deepen their knowledge and understanding of online behaviours and, in particular, how to prevent harm through continual learning resources, research and encouragement from all teachers.

6. Who is responsible for online safety and what are their responsibilities?

6.1 All staff

- Sign and follow the Staff Acceptable Use Policy in conjunction with this policy and read and understand the Safeguarding and Child Protection Policy, the Professional and Safe Conduct Policy and relevant parts of Keeping Children Safe in Education.
- Report any concerns regarding the safety or welfare of a child, no matter how small, to the designated safeguarding lead in line with the Safeguarding and Child Protection Policy.
- Report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Principal, DSL or other relevant person in line with this policy, other relevant

policies and internal academy procedures (including the Behaviour and Discipline Policy and Safeguarding and Child Protection Policy). This may include, for example, the Behaviour Lead in relation to the unacceptable use of technology.

- Maintain an awareness of current online safety issues and key guidance, through active engagement with training and updates.
- Model safe, responsible, and professional behaviours in their own use of technology at school and beyond.
- Embed online safety education in curriculum delivery wherever possible.
- Be vigilant in physically monitoring student internet and technology usage in line with this policy. This may include the use of personal technology, such as cameras, smart watches, and mobile phones on the academy site. Staff must not rely solely on monitoring software.
- Celebrate the benefits of technology with children, avoiding unnecessary scaremongering and the use of victim-blaming language.

6.2 The Executive Leadership Team:

- Take overall responsibility for data management and information security, ensuring provision follows best practice in information handling. This includes working with all relevant parties to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Provides active support across the Trust to ensure the DfE Cyber Security and Filtering and Monitoring Standards are met, and ensure the effective use, and procurement of, appropriate IT systems and services (including school-safe filtering and monitoring and protected email systems), and ensuring that technology, including cloud systems, is implemented according to child-safety first principles.
- Review and update this policy, Acceptable Use Policies and other related procedures on a regular basis, including ensuring that the policy is implemented consistently.
- Ensure all individuals, including staff, governors and trustees undergo safeguarding and child protection training and updates (including online safety), supporting those in governance to provide strategic challenge and maintain oversight into policy and practice. This includes ensuring that governors and trustees have an overview of online safety arrangements, including filtering and monitoring.

6.3 The Head of Safeguarding will:

- Monitor the effectiveness of online safety (including filtering and monitoring) within academies. This includes ensuring that academies have considered the number of and age range of children, those who are potentially at greater risk of harm and how often they access the IT system, along with the proportionality of costs versus safeguarding risks.
- Oversee the establishment, and ongoing effectiveness, of Online Safety Groups within each academy.
- Include online safety within safeguarding quality assurance and stakeholder voice activities, providing support and challenge to leadership teams and providing regular updates to the Executive Leadership Team and trustees (via the Safeguarding Review Group).

6.4 Principals will:

- Foster a strong culture of safeguarding where online safety is fully integrated into a whole school approach to safeguarding children.
- Support the updating of advice and guidance with regard to online safety, cyber security requirements, use of multi-factor authentication and similar.
- Oversee and support the activities of the designated safeguarding lead and ensure they work with technical colleagues to complete regular reviews of online safety.

- Ensure that all staff understand the importance of online safety and potential risks to children. They should ensure that staff understand this policy and that it is being implemented consistently throughout the academy.
- Ensure all staff undergo safeguarding training (including online safety) at induction and access regular updates.
- Take overall responsibility for data management and information security, ensuring that the academy's provision follows best practice in information handling, in line with Trust policies, procedures and professional advice.
- Work with the Data Protection Officer, DSL, Central Team and governors to ensure a compliant framework for storing data, helping to ensure that child protection is always put first, and data protection processes support careful and legal sharing of information.
- Better understand, review, and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards, through regular liaison with technical colleagues and the DSL – in particular, understanding what is blocked or allowed for whom, when, and how, as per Keeping Children Safe in Education 2023.
- Ensure the academy website meets statutory requirements, responding promptly to recommendations following internal or external reviews.

6.5 Governors will:

- Liaise with the DSL to report on how the academy is developing and maintaining links with local stakeholders and the wider school community in relation to online safety.
- Monitor the effectiveness of online safety provision through regular stakeholder engagement. This may include contributing to the work of the academy's Online Safety Group.

6.6 Trustees will:

- Maintain strategic responsibility for online safety, including filtering and monitoring, seeking regular assurance through the Safeguarding Review Group to ensure that academies are meeting filtering and monitoring standards.

6.7 The Designated Senior Lead (DSL) will:

- Take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure an effective, whole-school approach to online safety.
- Act as the named point of contact for all online safety incidents or issues and liaise with other members of staff and agencies as appropriate.
- Ensure that all members of the academy community have read and understood relevant Acceptable Use Policies.
- Oversee the development of Online Safety groups within each academy, chairing meetings to review the ongoing effectiveness of Online Safety. Through the Online Safety Group, DSLs will:
    - Review the effectiveness of online safety, at least annually, including the delivery and impact of the online safety policy.
    - Ensure online safety education is embedded across the curriculum and in line with the statutory guidance and the national curriculum.
    - Coordinate participation in local and national online safety events.
    - Monitor online safety incidents to identify trends and patterns and update the education response to reflect this need.
    - Review reports relating to filtering and monitoring, ensuring all incidents are responded to swiftly and appropriately and ensure that regular checks of the effectiveness of filtering and monitoring are completed and recorded.

- Ensure that online safety is promoted to staff, students, parents, and carers through a variety of channels and approaches.
- Work with relevant staff to ensure that data protection and data security practice is in line with legislation.
- Audit and assesses inset requirements for staff, support staff and governor online safety training.
- Ensure all staff undergo safeguarding and child protection training (including online safety) at induction and ensure that this is regularly updated. This must include filtering and monitoring to ensure everyone understands their roles.
- Ensure that online safety is integrated with other appropriate policies and procedures.
- Work with relevant staff to review protections for **remote-learning** procedures, rules and safeguards, where required.
- Work with behaviour colleagues to proactively respond to the unacceptable use of technology, including implementing escalating interventions in response to repeated incidents.
- Work with technical colleagues, leaders, the safeguarding governor and Trust leaders to develop a deeper understanding of filtering and monitoring, including better understanding, reviewing and driving the rationale behind systems in place, initiating regular checks and annual reviews, including providing support for devices within the home. Keep up to date with current research, legislation, and trends in online safety issues.

- Escalate online safety incidents to the relevant external parties e.g., the National Crime Agency's CEOP Safety Centre, Internet Watch Foundation, local Police, social services and parents/carers. Possible scenarios might include: Allegations against members of staff; cybercrime – hacking of school systems; allegations or evidence of grooming or exploitation; and allegations or evidence of online bullying in the form of threats of violence, harassment or a malicious communication.
- Be mindful of using appropriate language and terminology around children when managing concerns, avoiding victim blaming language.
- Ensure all online safety incidents are correctly categorised on CPOMS.
- Act 'in loco parentis' and liaise with websites and social media platforms to remove instances of illegal material or online bullying.
- Understand and make staff aware of procedures to be followed in the event of a serious online safeguarding incident.

6.8 Staff/contractors managing the technical environment:

- Provide and maintain a safe and secure technical infrastructure (including networks, infrastructure and hardware etc.) which supports safe online practices, ensuring learning opportunities are maximised and meets the DfE Cyber Security and Filtering and Monitoring Standards.
- Ensure systems are not open to abuse or unauthorised external access.
- Be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the internet, is secure.
- Defend the network and infrastructure of the academy, reviewing activity logs regularly.
- Ensure that users comply with basic access policies and that only trusted devices can connect to the academy network.
- Ensure that filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised. These checks should be recorded, with regular reports reported to leaders.

- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate these to leadership teams.
- To report to leadership teams any network intrusions or other threats to the network
- To ensure that any outsourced IT e.g., connectivity, maintenance, cloud-based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations.
- Promote basic cyber security practices within each academy e.g., locking computers when away from the desk and using secure passwords.
- External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.
- Provide technical support as required to ensure the development and implementation of appropriate online safety policies and procedures.
- Support home learning and remote teaching technologies as required.

6.9 PSHE /RSHE Leads:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the Personal Development, PSHE, Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.
- Work closely with the Computing Lead to ensure a complementary whole-school approach. This will ensure that the principles of online safety are covered at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. Curriculum Leads will be guided by the Education for a Connected World Framework.
- Focus on underpinning the knowledge and behaviours outlined in *Teaching Online Safety in Schools* in an age-appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to identify where pupils need extra support or intervention and to capture progress.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Pay particular attention to safeguarding provisions and online safety for home-learning and remote-teaching technologies.
- Ensure that the UKCCIS (2022) guidance '*Using External Visitors to Support Online Safety Education: Guidance for Educational Settings*' is followed when commissioning external speakers to complement the online safety curriculum.

6.10 Children and young people:

- Read the academy's Acceptable Use Policy and adhere to them.
- Respect the rights and feelings of others both on and offline.
- Seek help from a trusted adult or support network if things go wrong and support others who may be experiencing online safety issues. Examples may include a member of staff, CEOP, Child line etc.
- Contribute to the development of online safety and Acceptable Use policies through Student Voice.

- Be aware of and comply with academy policies for internet and mobile technology usage in the academy, including the use of personal items such as mobile phones.
- Follow basic cyber security practices within the academy e.g., locking computers when away from the desk, using secure passwords etc.
- Be aware that their internet use out of school on social networking sites is covered under the Acceptable Use Policy if it impacts on the school and/or its staff and students in terms of online bullying, reputation or illegal activities.

And at a level that is appropriate to the individual age, ability and vulnerabilities:

- Sign the academy's Acceptable Use Policy.
- Take responsibility for keeping themselves and others safe online.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assess the personal risks of using any particular technology and behave responsibly to limit those risks.
- Work with the relevant staff to follow **remote-learning** procedures, rules and safeguards, where applicable.

6.11 Parents and carers:

- Read their child's Acceptable Use Policy and support and encourage them to adhere to it and to adhere to it themselves as needed.
- Sign the academy's Acceptable Use Policy upon enrolment at the academy, indicating agreement regarding their child's use and their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.
- Discuss online safety issues with their children, supporting the academy in their online safety approaches and reinforcing appropriate safe online behaviours at home.
- Role model safe and appropriate uses of new and emerging technology.
- Identify changes in their child's behaviour which indicate that their child is at risk of harm online.
- Seek help and support from the academy, or other appropriate agencies, if they have concern.
- Use school systems safely and appropriately.
- Take responsibility for their own awareness and learning in relation to online risks for their children.

7. Procedures

7.1 Systems

7.1.1 School computer systems will be configured to ensure the teaching and learning requirements of the school are met whilst ensuring online safety is maintained.

7.1.2 Risk assessments are completed when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

7.1.3 The system will be compliant with the academy, Trust, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

7.1.4 Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

7.1.5 IT use will be monitored.

7.2 Filtering and Monitoring

7.2.1 Each academy will do all they reasonably can to limit children's exposure to online risks, by employing effective filtering and monitoring, and regularly reviewing the

effectiveness. Levels of filtering and monitoring will be informed by the academy's Prevent Risk Assessment, as well as an understanding of the number and age range of children, those who are potentially at greater risk of harm and how often they access the IT system, along with the proportionality of costs versus safeguarding risks. Steps will be taken to avoid over blocking, so as to not unreasonably impact teaching and learning.

7.2.2 Leaders and relevant staff will have an awareness and understanding of the provisions in place and manage them effectively.

7.2.3 Filtering and monitoring reports and logs will be examined regularly and used to inform targeted intervention with identified students and inform the online safety curriculum.

7.2.4 Any filtering incidents are examined, and action taken and recorded to prevent a reoccurrence.

7.2.5 The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

7.3 Network security

7.3.1 All users will have clearly defined access rights to academy technical systems and devices.

7.3.2 All users will be provided with a username and secure password by school IT staff. Users are responsible for the security of their username and password and will not share the password with others.

7.3.3 The Network Manager and Principal/other designated senior person will have access to the main administrator password.

7.3.4 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

7.4 Use of images and videos

7.4.1 The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.

7.4.2 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g., social media sites.

7.4.3 Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press.

7.4.4 In accordance with guidance from the ICO, parents/carers can take videos and digital images of their children at academy events for their own personal use, but should not be made publicly available where other students are involved in the digital image or video.

7.4.5 Students must not take, use, share, publish or distribute images of others without their permission.

7.4.6 Staff (including volunteers, governors, supply staff and contractors) must not use their personal mobile phone to capture photos or videos of pupils.

7.5 Data Protection

7.5.1 Personal data will be recorded, processed, transferred and made available according to the Trust Data Protection Policy (TPO/STA/25) and in compliance with the Data Protection Act (2018) and any subsequent updates.

7.6 Social Media

7.6.1 Governors, staff, students and volunteers are expected to comply with the Professional and Safe Conduct Policy (TPO/STA/10)

7.7 Managing email

7.7.1 Pupils, staff and governors may only use their academy/Trust email accounts for educational purposes and for any official communication. The use of personal email addresses for any official business is not permitted.

7.7.2 Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods. Only data that needs to be shared should be.

7.7.3 Members of the school community must report any offensive communication immediately to the DSL.

7.7.4 Emails sent internally should be professionally written and used in line with the acceptable use policy and communications charter, minimising emails wherever possible. This is an important element in managing staff workload and enhancing communication.

7.7.5 Emails sent to external organisations should be written carefully and authorised before sending, in the same way that a letter written on school headed paper would be. Authorisation is not required for staff who routinely communicate with external agencies as part of their role, e.g., DSLs.

7.7.6 Where academies have a dedicated email for reporting wellbeing and pastoral issues, the inbox should be managed by designated and trained staff.

7.7.7 School email addresses must not be used for setting up personal social media accounts.

7.7.8 All staff must follow the guidance contained within the *BWT Electronic Communications – Use and Management Guidance.*

7.8 Acceptable Use Policy

The Acceptable Use Policy contains more in-depth information with regards to the expectations of students and staff.

8. Educating students about online safety - curriculum

8.1 Students will be taught about online safety as part of the curriculum. This includes the Relationships Education, Relationships and Sex Education, Health Education and the Computing Curriculum. Online Safety will also be addressed through the wider curriculum.

8.2 In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Critically analyse information to make a judgement about probable accuracy and understand why it is important to make their own decisions regarding content

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

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

Academies will use a range of activities to raise pupils' awareness of the dangers that can be encountered online including assemblies, Awareness Days, external speakers etc.

8.3 When planning the curriculum, schools will carefully consider how to tailor the online safety curriculum to ensure that it meets the needs of students who may be more vulnerable online. This may include children who are in care, or children with special educational needs, through triangulation with the Designated Teacher and SENCO. Schools will also assure themselves of the quality of external resources and external visitors commissioned to speak to children about online safety.

9. Educating parents and carers about online safety

9.1 The Trust 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 digital technology. It is important that parents and carers support their children with the procedures, rules and safeguards that are in place for remote learning, where this may be required.

9.2 Academies will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via the website. This policy will also be available to parents via the website.

9.3 Parents and carers are requested to read the academy's Acceptable Use Policy for Students and discuss it with their children. We also request parents read and discuss online safety information as part of the Home School Agreement with their children.

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

10. Use of mobile phones and smart technology

10.1 Brooke Weston Trust recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G). This access means some children, whilst at school, may experience or perpetrate sexual harassment, bullying, online coercion or control. Children may also share indecent images consensually or non-consensually, and may view or share pornography of other harmful content. Each academy will respond to such issues in line with the Behaviour and Discipline Policy and Safeguarding and Child Protection Policy.

10.2 Each academy will have its own approach to the use of mobile phones in school. This will be clearly communicated to students, staff, parents/carers and volunteers.

10.3 Any use of mobile phones must be in line with the relevant acceptable use agreements.

10.4 Staff must not use their personal number phone to communicate with students or their parents/carers, unless in the most exceptional circumstances and where there is no other alternative, and only with the approval of a Principal, the Head of Safeguarding or Director of Education. Staff must not share their personal mobile numbers with students under any circumstances.

10.5 Any breach of the acceptable use agreement by a student or members of staff may trigger disciplinary action, in line with the Behaviour and Discipline Policy and other relevant policies, and in the case of a students may result in the confiscation of their device.

11. Examining Electronic Devices

11.1 Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

11.2 Staff who have been authorised by the Principal may examine any data or files on an electronic device they have confiscated as a result of a search, if there is good reason to do so.

11.3 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Undermine the safe environment of the school
- Disrupt teaching
- Be used to commit an offence

11.4 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this 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 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 (see BWT CPOMS Toolkit).

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

11.5 Any searching of pupils 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

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

12 Policy Review

12.1 This policy will be monitored as part of the academy's annual internal review and reviewed annually or a required by legislation changes.

12.2 An up-to-date copy of the policy will be available on the Trust website.

Appendix A – Cyber Crime

Cybercrime is a broad term used to cover all crimes that: take place online, are committed using computers or are facilitated by online technology. Common attacks include:

- Ransomware
- Insider threats
- Phishing
- Mandate fraud

The Education and Skills Funding Agency has produced detailed guidance on *Cyber Crime and Cyber Security: A Guide for Education Providers (2023).*

Cybercrime can be committed by children. The National Police Chief's Council has produced guidance on *When to Call the Police: Guidance for Schools and Colleges*. When responding to incidents involving students, the academy should first establish:

- What has happened?
- Who is involved?
- Is this part of a pattern of behaviour?
- Are there any safeguarding concerns? If yes— Refer to Keeping Children Safe in Education (September 2023) and follow the Safeguarding and Child Protection Policy
- Are there any aggravating factors?
    - Did this incident cause any disruption to the school? E.g., loss of access to website and online learning platforms or school communication networks disrupted.
    - Did the school suffer a loss of data or corruption of files?
    - Did the school suffer loss of teaching time resulting on an impact on other students?
    - Is there a hate element?
    - Have they expressed any ideological motivation or reason for their actions?
    - Is there evidence of escalating behaviour? Or previous incidents of a similar nature?
    - Is the behaviour related to gang activity or an Organised Crime Group?
    - Do the young people involved have any additional relevant vulnerabilities?

If aggravating factors are present, the school should report the incident to Action Fraud and/or the Police, in line with *When to Call the Police: Guidance for Schools and Colleges*.

Appendix B – Relevant Legislation

Academies should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programmes;
- Deny access to authorised users.

Academies may wish to view the National Crime Agency website which includes information about "Cybercrime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:
Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives and business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure.
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they must follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn

their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g., YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. The Sexual Offences Act was also amended by the Voyeurism (Offences) Act 2019, to include offences of voyeurism.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015
Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Appendix C - Online Safety guidance and resources

Helpful websites and information

- https://nationalonlinesafety.com/about
- https://www.ceop.police.uk/safety-centre/
- 2491596 C&YP schools guides.indd (npcc.police.uk)
- https://www.iwf.org.uk/
- https://www.actionfraud.police.uk
- https://www.lucyfaithfull.org.uk/
- https://www.mariecollinsfoundation.org.uk/

For parents

- https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/
- https://educateagainsthate.com/parents/
- https://nationalonlinesafety.com/guides
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting
- https://www.internetmatters.org/
- https://www.net-aware.org.uk/

For students

- https://www.thinkuknow.co.uk
- https://www.ceop.police.uk/safety-centre
- www.childline.org.uk

Curriculum

- https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf