Brown's School
E-Safety Policy

Full Name of Policy	E-Safety Policy
Date of Approval	September 2023
Date of Next Formal Review	September 2024

Brown's School
Empowering Tomorrow's People

Introduction

This policy has been developed in accordance with the Government guidance, Teaching Online Safety in School, 2019, Education for a Connected World, UKCIS 2020 and Safeguarding in the Context of Access to Technology and Use of Social Media, Bromley Safeguarding Children Board, 2017 (now Bromley Safeguarding Children Partnership).
It takes into account the DfE statutory guidance, Keeping Children Safe in Education 2023 and Working Together to Safeguard Children 2018 (including updates in February 2019 and December 2020).
Brown's School recognises that that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential online harm. This policy has been written with the particular needs of Brown's pupils in mind. Staff are aware that students with learning difficulties are vulnerable and may expose themselves to greater risks online and that children with special educational needs are more likely to be persistently cyberbullied over a prolonged period of time. Therefore, we recognise that our pupils may require additional teaching, including reminders, prompts and further explanations to reinforce their existing knowledge and understanding of ICT issues and appropriate and safe online behaviour. It is crucial that we explicitly teach our pupils that online actions can have offline consequences.

The Headteacher and Senior Leadership Team have taken the decision that, due to the nature of our pupils' difficulties and with the objective of keeping everyone safe, pupils are not allowed access to their mobile phones during the school day.

Children, young people and adults interact with technologies such as mobile phones, games consoles and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults at risk. The school identifies that the internet and associated devices are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks and the Headteacher is aware of the school's responsibility to safeguard its pupils online as well as offline.

Brown's School aims to empower and educate its pupils so that they are equipped with the skills to make safe and responsible decisions when using the internet and technology. Pupils will be taught to use the internet in a considered and respectful way and will develop their resilience so that they can manage and respond to online risks.

All members of staff understand that for young people there is no separation between 'real life' and the 'online world' and that technology is a significant component in many safeguarding and wellbeing issues. Staff are aware that children and young people are at risk of abuse online as well as face to face and, in many cases, abuse will take place concurrently, sometimes involving each other.

All members of staff are aware of the importance of good e-safety practice in the classroom in order to educate and protect the pupils in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. The school has a Social Media Policy and Code of Conduct for staff to refer to.

The E-safety Policy is essential in setting out how the school plans to develop and establish its e-safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Brown's School
Empowering Tomorrow's People

Policy Aims

The purpose of Brown's School's E-safety Policy is to:

- Safeguard and protect all members of Brown's School 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.

Brown's School identifies that the issues classified within online safety are considerable but can be broadly categorised into three 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 which increases the likelihood of, or causes, harm.

Monitoring and Review

- As technology evolves and changes rapidly, Brown's School will review this policy annually, but will revise it following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- The school will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is constantly applied.
- The Headteacher is the e-safety coordinator and will be informed of any online safety concerns to ensure oversight of online safety.
- Any issues identified will be incorporated into the school's action planning.

Roles and Responsibilities

The Headteacher

The Headteacher holds overall lead responsibility for online safety and coordinates e-safety for the school. The Headteacher recognises that all members of the community have important roles and responsibilities to play with regards to online safety and liaises regularly with the school's computer science coordinator and technical support team.

The Headteacher will:

- Create a whole school culture that incorporates online safety throughout all elements of school life.
- Carry out an annual review of the school's approach to online safety, supported by an annual risk assessment that considers and reflects the risks pupils face.
- Ensure that online safety is considered whilst planning the curriculum, training staff, in the role and responsibilities of the school's Designated Safeguarding Leads (DSLs) and any parental engagement.
- 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 appropriate and up-to-date policies regarding online safety are in place which address the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Ensure robust reporting channels are in place regarding online concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Ensure that staff are trained so that they have an awareness of a range of online safety issues and feel confident to identify online safety concerns and take appropriate action.

- ∞ Audit and evaluate online safety practice to identify strengths and areas for improvement.
- ∞ Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety.
- ∞ Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.
- ∞ Access regular and appropriate training and support to ensure they understand the risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.

The Designated Safeguarding Leads (DSLs)
George Mitchell and Denise Mitchell are the School's DSLs and they will:

- ∞ Ensure appropriate referrals are made to relevant external agencies, as appropriate.
- ∞ Work to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated whole school approach is implemented.
- ∞ Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day, Anti-bullying Week (including cyberbullying), etc.
- ∞ 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 school's safeguarding recording mechanisms.
- ∞ Monitor online safety incidents to identify gaps and trends and use this data to update the school's policies and procedures.
- ∞ Report online safety concerns, as appropriate, to the Senior Leadership Team (SLT) and the Governing Body.
- ∞ Work with all staff to review and update online safety policies and procedures on a regularly basis at staff meetings.

Staff
It is the responsibility of all staff to:

- ∞ Contribute to the development of online safety policies.
- ∞ Read and adhere to the E-safety Policy, Social Media Policy and Acceptable Use Policy (AUP).
- ∞ Take responsibility for the security of school systems and the data they use or have access to.
- ∞ 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 children in their care.
- ∞ Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.

Technical Support

Technical support is provided by an independent service and managed by David Greenbury. He is responsible for:

- Providing technical support and perspective to the Headteacher and SLT, particularly in the development and implementation of appropriate online safety procedures.
- Implementing appropriate security measures (including passwords and encryption) to ensure that the school's IT system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensuring that filtering and monitoring procedures are applied and updated on a regular basis.
- Ensuring that appropriate access and technical support is given to the Headteacher and DSLs to the school's filtering and monitoring systems to enable them to take appropriate safeguarding action if and when required.

Pupils

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

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school's AUP for pupils.
- Respect the rights and feelings of others both on and offline.
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult if there is a concern online and support others that may be experiencing online safety issues.

Parents and Carers

It is the responsibility of parents and carers to:

- Read and sign the school's AUP for parents/carers and encourage their children to adhere to them.
- Support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home. The school promotes this by sending home regular e-safety bulletins.
- Role model safe and appropriate use of technology and social media.
- Seek help and support from the school or other agencies, if they or their child, encounter online issues.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies used by their children.

Teaching and Learning

It is important to state that as a school we are committed to delivering a full computer science curriculum, which includes internet use, for all our students in the safest possible way. Developing effective practice in using the internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the internet. Respect for copyright and intellectual property rights and the correct use of published material should be taught.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Pupils use the internet widely outside of school and need to learn how to evaluate internet information and to take care of their own safety and security.
- The purpose of internet use in school is to raise educational standards by encouraging independent learning.
- The school's internet access will be designed to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The school will ensure that the copying and subsequent use of internet-derived materials by staff and pupils complies with copyright law.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupil's age and ability.
- Pupils will be educated in the effective use of the internet in research.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

<u>How the School Provides E-Safety Education</u>

Pupils' Curriculum Teaching

- Ensuring that the curriculum and whole school approach is developed in line with the UK Council for Internet Safety, UKCIS, 'Education for a Connected World Framework' and DfE, 'Teaching online Safety in school' guidance 2020.
- Teaching e-safety as part of the computer science teaching unit; how to judge the validity of website information, how to remove cyber bullying, computer usage and the law, how to spot and remove viruses, why copyright is important.
- Teaching e-safety as part of a Personal, Social, Health and Economic (PSHE) teaching unit; how to stay safe online and have healthy online relationships; how to deal with cyber bullying (including bullying of a sexual nature), how to report cyber bullying, the social effects of spending too much time online, etc.
- Teaching e-safety as part of pastoral care; form time activities, assemblies, tutorial opportunities and 1:1 sessions with the pastoral care team.

- Reinforcing online safety principles in other curriculum subjects, as appropriate, and whenever technology or the internet is used on site.

- The computer science coordinator will liaise with the DSL when planning online safety lessons or activities so that the DSL can advise on any known safeguarding cases and ensure support is in place for any pupils who may be impacted by the content

- E-Safety events in school such as Safer Internet Day and Anti-bullying week (including online bullying)

- Displaying posters in school to promote online safety.

- Ensuring that any educational resources used are appropriate to pupils' learning. Staff should check with the Headteacher if they require clarification.

Parents and Carers - Information, Presentation and Events

- An AUP for Parents is sent to all parents/carers. It is expected that parents/carers will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home by signing the AUP.

- E-safety information is directly delivered to parents by means of regular bulletins.

- The school holds an annual parent workshop on *Keeping Children Safe Online* to provide parents with updates and useful information to implement with their children.

Vulnerable Pupils

- Brown's School recognises that its pupils are vulnerable online due to their special educational needs. However, there are some pupils, for example Looked After Children and children who have a social worker, who may be more susceptible or may have less support in staying safe online.

- The School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.

Safe Use of Technology

Classroom Use
Brown's School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which includes search engines and educational websites
- Email
- Digital cameras, web cams and video cameras

- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommendation for use at home.
- The school will use appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our school community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils will be supervised by staff at all times when using the internet.

Brown's School
Empowering Tomorrow's People

Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.

- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

Filtering and Monitoring

The Headteacher and SLT have ensured that the school has age and ability appropriate filtering and this is managed by an independent IT consultant, David Greenbury. The school has a firewall subscription with FortiGate. *FortiGate NGFW is the world's most deployed network firewall, delivering unparalleled AI-powered security performance and threat intelligence, along with full visibility and secure networking convergence.*
We can design the filter and tailor it to block specific sites or filter key words. For example the filter will block any inappropriate sites such as pornography, gambling, extremism or terrorism content, and social media. This list is not exhaustive.
The school also uses the NetSupportDNA for Schools programme. NetSupport allows for internet monitoring and restrictions to prevent access to inappropriate websites, control access to content on memory sticks, and trigger alerts if violations occur. Within the keyword and phrases monitoring tool, if a safeguarding keyword (in any language) is matched anywhere on the network, the event is captured immediately (available as a log, screenshot, or screen recording) and provides a full background to the safeguarding incident. The data captured is securely stored on the school network (LAN) and only Designated Safeguarding Leads can access the information. NetSupport also allows the class teacher to be able to monitor all screens in use in real time.

- The Headteacher and SLT are aware of the need to prevent 'over blocking', as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding whilst remaining vigilant due to the special educational needs/vulnerability of its pupils.

- The Headteacher and SLT will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

- If pupils discover unsuitable sites, they will be required to:
  - Turn off monitor/screen and report the concern immediately to a member of staff.
  - The member of staff will report the concern to the DSL
  - The DSL will contact Techinical Support and record and escalate it as appropriate
  - Parents/carers will be informed of filtering breaches involving their child.
  - Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation (IWF), Child Exploitation and Online Protection (CEOP) and/or the police.

Staff will also monitor internet use on all school owned or provided internet enabled devices. This is achieved by:

- physical monitoring (supervision)
- monitoring internet and web access (reviewing logfile information)

All users will be informed that use of the school's systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation. If a concern is identified via monitoring approaches the DSL will respond in line with the Child Protection Policy.

Brown's School
Empowering Tomorrow's People

Risk Assessment

Brown's School accepts that it is not possible to completely remove the risk that pupils might access unsuitable materials via the school system but will take all reasonable precautions to ensure that users access only appropriate material. The school cannot accept liability for the material accessed, or any consequences resulting from internet use.

The school will undertake a regular e-safety audit to establish if the E-safety Policy is adequate and if its implementation is adequate.

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.

Security and Management of Information Systems

The school takes appropriate steps to ensure the security of its information systems, including:

- Virus protection which is updated regularly.
- Sending sensitive information via Egress.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Preventing, as far as possible, access to websites or tools which could compromise the school's systems, including anonymous browsing and other filtering bypass tools.
- The appropriate use of logins and passwords to access the school network. This is enforced for all users. Users are required to use strong passwords for access into the system, not share passwords or login information with others or leave password/login details where others can find them. Users should not login as another user at any time.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Managing the Safety of our Website

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

Brown's School
Empowering Tomorrow's People

Managing Email

Email is an essential means of communication for both staff and pupils but should be managed appropriately by staff for our pupils. Email use by pupils is limited to when it is required for formal qualifications. Email accounts for pupils are created by staff and parental permission is sought. In the school context email should not be considered private and Brown's School reserves the right to monitor email. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Access to the school's email systems will always take place in accordance with data protection legislation and in line with other policies, including the Code of Conduct.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Sensitive or personal information will be sent via Egress.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the school community will immediately tell the Headteacher or DSL if they receive offensive communication via school email and this will be recorded in our safeguarding files.

Publishing Images and Videos Online

Brown's School draws upon the guidance provided by BSCP relating to the use of photographic images of children (appendix 1). The school needs to comply with the Data Protection Act 1998 and Freedom of Information Act 2000, as well as preserving the safety of children.

- Images of a pupil should not be published without the parent's or carer's written permission. Browns School asks parents/carers to sign a form giving permission for images to be taken as part of its admissions procedure. The form indicates that images will be used appropriately.
- Images or videos that include pupils will be selected carefully and staff must be aware of the potential for these images to be misused for pornographic or grooming purposes.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Consent from staff, or any other adults who may appear in a photograph or DVD is also required.
- Images will be securely stored and used only by those authorised to do so. Photographs will be stored electronically in a secure area.
- Pupils are not allowed to have their mobiles phones with them in school during the day. Pupils are allowed to bring them into school but they are given to staff first thing in the morning and locked away safely. Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with inappropriate capture, use or distribution of images of pupils or staff
- Pupils work can only be published externally with parents' permission.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

Brown's School
Empowering Tomorrow's People

Social Media

The school has a separate Social Media Policy.

All members of the school community need to be aware that the internet has social networks which allow individuals to publish unmediated content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with pupils or personally. Staff should refer to the school's Social Media Policy.

- The expectations regarding safe and responsible use of social media applies to all members of the Brown's School community.
- The term 'social media' may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chat rooms and instant messenger.
- The use of social media during school hours for personal use is permitted for staff during lunchtimes and breaktimes only – never in the classroom.
- Pupils do not have access to social media sites during the school day.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the SLT in this scenario.
- Newsgroups will be blocked unless a specific use is approved by the SLT.
- Parents will be advised that the use of social networking spaces outside school brings a risk of dangers for young and vulnerable groups.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes and are moderated by staff.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- The personal use of social networking, social media and personal publishing sites by staff will be discussed as part of staff meetings.
- Concerns regarding the online conduct of any member of Brown's School community on social media will be reported to the Headteacher and be managed in accordance with the Anti-bullying ,Managing Allegations against Staff, Behaviour, Code of Conduct and Child Protection policies

Brown's School
Empowering Tomorrow's People

Mobile Phones and Personal Devices

Due to the widespread use of personal devices it is essential that Brown's School takes steps to ensure mobile phones and devices are used responsibly at school. The Headteacher and SLT are aware that unrestricted and unlimited access to the internet via mobile phone networks can result in some children, whilst at school, harassing their peers, including sexually, via their mobile phone and other smart technology devices. The school's Headteacher and SLT also feel that it is essential that pupil use of mobile phones does not impede teaching, learning and good order in classrooms. With both of these factors in mind, it is school policy that all electronic devices are collected before school starts at the beginning of the day at the school gate and returned to the pupils as they are leaving the school premises at the end of the school day. Pupils are allowed access to personal devices during reward time (Golden Time) and this is closely supervised by a responsible adult. During the COVID pandemic pupils put their phones in a sanatised bag and into a box at the gate.

Staff are given clear boundaries on professional use. Staff are expected to use the school phone network to contact pupils and parents with the exception of the school's Business Manager/ DSL who has the use of a school mobile phone. Staff can request that texts are sent to parents and/or pupils on the school mobile if necessary.

- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school such as toilets and where children are changing.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community. Any breach will be dealt with in line with our School Discipline/Code of Conduct policies.
- All members of Browns School 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, Child Protection or Code of Conduct policies.
- Staff will keep mobile phones and personal devices switched off during lesson times and will not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances.
- Pupils are not allowed their mobile phones during the school day. If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone.
- Mobile phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Parents are advised to contact their child via the school office.
- Parents/carers and visitors, including volunteers and contractors, should ensure that mobile phones and personal devices are only used away from children. Members of staff are expected to challenge visitors if they have concerns and inform the DSL of any breaches of our policy.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of school in a professional capacity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

.

Responding to Online Safety Incidents

- All members of the school community will be informed about the procedure for reporting e-safety concerns including breaches of filtering, illegal content and peer on peer abuse, including cyberbullying, youth produced sexual imagery (sharing of nude or semi-nude images), online sexual violence and harassment, online abuse and exploitation.

- The DSLs will be informed of any e-safety incidents involving child protection concerns, which will then be escalated appropriately.

- The DSLs will record all reported incidents and actions taken in the serious misbehaviours log or child protection files.

- If the school is unsure how to proceed with an incident or concern, the DSLs will seek advice from Children's Social Care (MASH) or the Bromley LADO.

- Where there is a concern that illegal activity has taken place, the Headteacher or DSsL will contact the police using 101 (or 999 if there is an immediate danger or risk of harm).

- The school will manage pupil incidents in accordance with the school's Behaviour Policy. Appropriate sanctions and pastoral support will be applied to students as appropriate.

- Any issues involving staff will be referred to the Headteacher and dealt with according to the school's staff disciplinary procedures. Concerns about the Headteacher should, in the first instance, be referred to the Proprieter of the school, Ms Elaine Lovett, 07584 415151 and the Chair of Governors, Ms Sarah Mortiboys: sarahmortiboys@brownsschool.co.uk.

- The school will inform parents/carers of any incidents of concerns as and when required.

- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with the school to resolve issues.

- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Brown's School
Empowering Tomorrow's People

Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children

- Peer on peer abuse, including online sexual abuse and harassment, will not be tolerated. Brown's School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community and for repeat victimisation in the future if abusive content continues to exist somewhere online. To help minimise concerns, the school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual incidents by implementing a range of age and ability appropriate educational methods as part of our curriculum. The school will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between pupils, youth produced sexual imagery (sharing of nude and semi-nude images) and online abuse and exploitation and will put further support in place through the school's therapy team, including the Clinical Psychologist, if appropriate. The school will respond to concerns of a sexual nature between children, regardless of whether the incident took place on the school premises or using school equipment. Staff should immediately notify the DSL if they become aware of a case of an online sexual incident and the DSL will seek advice and refer to outside agencies such as Children's Social Care (CSC) and/or the police, if appropriate. The handing of any incidents will be reviewed to ensure that best practice was implemented and that policies/procedures are appropriate.

The school has a separate Peer on Peer Policy which outlines our response to peer on peer abuse, including sexual violence and harassment.

- The Headteacher and SLT have accessed and understood the guidance 'Sexual violence and sexual harassment between children in schools and colleges', DfE 2018 and part 5 of Keeping children safe in education 2021.

- Staff recognise that sexual violence and sexual harassment between children can take place online including non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats and upskirting, which typically involves taking a picture under a person's clothing with the intention of obtaining gratification or causing the victim humiliation, distress or alarm. Upskirting is a criminal offence.

- If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'Searching Screening and Confiscation' 2018 advice.

- Appropriate sanctions will be implemented in line with the school's Behaviour Policy.

- Parents/carers will be informed, if appropriate, about the incident and how it is being managed.

- If the concern involves children and young people at a different educational setting, the DSLs will work in partnership with other DSLs to ensure that appropriate safeguarding action is taken. If a criminal offence has been committed, the DSLs will discuss this with the police first to ensure that investigations are not compromised.

Youth produced sexual imagery/sharing nude and semi-nude images/videos (also referred to as 'indecent imagery' and 'sexting').

Brown's School
Empowering Tomorrow's People

The sharing of nudes and semi-nudes is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This can be via social media, gaming platforms, chat apps or forums. The motivations for taking and sharing these are not always sexually or criminally motivated. However, if it involves adults sharing nudes or semi-nudes of under 18 year olds, it is a form of child sexual abuse and will be referred to the police by the school as a matter of urgency. The school recognises that it is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

- Brown's School recognises that the sharing of nudes and semi-nudes by pupils is a safeguarding concern and all incidents which come to the attention of staff will be reported to and dealt with by the DSLs.

- The DSL will follow the advice as set out in the non-statutory advice by UKCIS 2020 ''Sharing nudes and semi-nudes: advice for education settings working with children and young people' and' Sharing nudes and semi-nudes: how to respond to an incident''

- The DSLs understand that consensual image sharing, especially between older children of the same age may require a different response as it may not be abusive, however young people still need to know that it is illegal – whilst non-consensual is illegal and abusive.

What staff should do if an incident comes to their attention:

- Report immediately to one of the school's DSLs.
- Do not send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request pupils to do so as this is illegal.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person(s) involved in the incident to disclose information regarding the imagery as this is the responsibility of the DSLs.
- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other parents/carers.
- Do not say or do anything to blame or shame any young person involved.
- Explain to the young person that you need to report it and reassure them that they will receive support and help from the DSLs

- The DSLs will not view any suspected nudes or semi-nudes, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed by the DSLs and any decision making will be clearly documented.
- If the DSLs are made aware of an incident involving the creation or distribution of nudes or semi-nudes, she will respond in line with UKCIS guidance and store any devices containing potential nude or semi-nude images securely. If content is contained on pupils' personal devices the DSLs will manage this in accordance with the DfE 'Searching Screening and Confiscation' advice. If a potentially indecent image has been taken or shared on the school's network or devices, the school will act to block access to all users and isolate the image.
- The DSL will carry out a risk assessment in line with UKCIS guidance which considers the age and vulnerability of the pupils involved, including the possibility of carrying out relevant checks with outside agencies.
- The DSLs will inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- The DSLs will make a referral to CSC and/or the police, if appropriate.
- Sanctions will be implemented in accordance with the school's Behaviour Policy and care will be taken not to further traumatise victims where possible.
- The DSLs will consider the deletion of images in accordance with UKCIS guidance. Images will only be deleted once the DSLs have 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.

Brown's School
Empowering Tomorrow's People

Online Abuse and Exploitation (including child sexual abuse and sexual or criminal exploitation)

- Brown's School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, is a safeguarding issue and all concerns will be reported to and dealt with by the DSLs. If appropriate, the DSsL will seek advice/refer to outside agencies such as CSC and/or the police.

- The school will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target children and young people, and understand how to respond to concerns.

- The school will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and is available to pupils and other members of the school community.

- Parents/carers will be informed about the incident and how it is being managed.

- The school will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on the school's premises or using school equipment or personal equipment.

- Where possible and appropriate pupils will be involved in decision making and if appropriate, they will be empowered to report concerns themselves with support, for example through CEOP.

Indecent Images of Children (IIOC)

- Brown's School will ensure that all members of the community are made aware of the possible consequences of accessing indecent images of children, as appropriate to their age and ability.

- The school will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place offsite.

- If made aware of incidences of IIOC the DSL will store any devices involved securely and immediately inform appropriate organisations, such as the IWF (via www.iwf.org.uk) and Police.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, the DSL will be informed. The DSL will ensure that the URLs (webpage address) which contain the suspect images are reported to the IWF via www.iwf.org.uk, ensure that any copies that exist of the image, for example in emails, are deleted and report concerns, as appropriate, to parents/carers. Concerns about the Headteacher should be referred to the Chair of Governors, Ms Sarah Mortiboys: sarahmortiboys@brownsschool.co.uk.

- If made aware that indecent images of children have been found on a device provided by the school, the DSL will be informed. The DSL will ensure that the URLs (webpage address) which contain the suspect images are reported to the IWF via www.iwf.org.uk, inform the police via 101 (or 999 if there is an immediate risk of harm, and CSC, as appropriate.

- The school will only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police. Parents/carers will be informed, as appropriate.

- If made aware that a member of staff is in possession of indecent images of children on school provided devices, the Headteacher will be informed in line with the school's Managing Allegations against Staff Policy. The LADO will be informed and devices will be quarantined until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Brown's School. Full details of how the school will respond to cyberbullying are set out in our Anti-bullying Policy.

Online Hate

- Online hate content, directed towards or posed by, specific members of the school community will not be tolerated at Brown's School and will be responded to in line with existing policies, including Child Protection, Anti-bullying and Behaviour.

- All members of the school community are advised to report online hate in accordance with relevant policies and procedures.

- The school will contact the police if a criminal offence is suspected.

Online Radicalisation and Extremism

- Brown's School will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

- If any member of staff is concerned that a pupil may be at risk of radicalisation online, the DLS will be informed immediately and action will be taken in line with our Extremism and Anti-Radicalisation and Child Protection policies.

- If the school is concerned that a member of staff may be a risk of radicalisation online the Headteacher will be informed immediately and action will be taken in line with the Child Protection and Allegations Policies

Review of the E-safety Policy with Staff

It is important that all staff feel confident to use new technologies in teaching and the school's E–safety Policy will only be effective if all staff subscribe to its values and methods. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies at weekly staff meetings and during designated inset days. Staff are made aware of their responsibility to maintain confidentiality of school information.

- The E–safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and pupils, the school will implement its AUPs.

- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.

- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities

Brown's School
Empowering Tomorrow's People

Parent Support

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school is able to help parents plan appropriate, supervised use of the internet at home and educate them about the risks.

- ∞ Parents will be advised that the school's E-safety Policy is available from the school office and on the school's website
- ∞ Parents will be expected to read and sign the school 's AUP and discuss its implications with their children.
- ∞ Information and guidance for parents on e–safety will be made available to parents in a variety of formats
- ∞ Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the internet will be made available to parents
- ∞ A partnership approach to e-safety at home and at school with parents will be encouraged. Parents are offered the opportunity to liaise with the school's technical support department to implement parental controls

National Links and Resources for Pupils, Staff and Parents/Carers

CEOP: www.ceop.police.co.uk
www.thinkuknow.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk
UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
Report Harmful Content: https://reportharmfulcontent.com/
360 Safe Self-Review tool for schools: www.360safe.org.uk
Childnet: www.childnet.com
Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speakup/guidance-and-training-for-schools-and-professionals
Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
Internet Matters: www.internetmatters.org
Parent Zone: https://parentinfo.org
NSPCC: www.nspcc.org.uk/onlinesafety
Childline www.childline.org.uk
Net Aware: www.net-aware.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
The Marie Collins Foundation: www.actionfraud.police.uk
Get Safe Online: www.getsafeonline.org

Brown's School
Empowering Tomorrow's People

Reviewed in Staff Meeting

Person responsible for editing: George Mitchell in September 2022

_____Signature

_____Date

_____Headteacher

_____Date

This policy will be reviewed in September 2023

Brown's School
Empowering Tomorrow's People

Bromley Safeguarding Children Board
Guidance On Using Photographic Images of Children

Introduction

This guidance has been produced to assist educational establishments, and other organisations who work with children and young people, in forming their own policies and procedures regarding the safe photography and the video recording of children and young people.

It is important that schools take practical steps to ensure that pictures and images of children taken, not only by members of the press, school staff, but also by parents/carers, are done in a way that reflects the protective ethos of the school.

Establishments using photographic images of children and young people need to comply with the Data Protection Act 1998 and Freedom of Information Act 2000 as well as preserving the safety of children.

- Always ask for parental/carer consent for photographs to be taken of children, who are under the age of 18 years of age, while in school or on school activities. It is suggested that parents/carers are asked to sign a section of the school's admissions form giving permission for images to be taken, but that also the form indicates that images will be used appropriately. Parents may also be written to before individual trips or events requesting permission with a returnable signed permission slip. Images should not be displayed on websites, in publications or in a public place without consent. The definition of a public place includes areas where visitors to the school have access.
- If two parents disagree over consent for their child to appear in photographs or in DVD recordings, then it has to be treated as if consent has not been given. Likewise, if the parents give consent but the child does not, then it is safer to assume that consent has not been given.
- Consent from staff, or any other adults, who may appear in the photograph or DVD is also required.
- Many school activities involve recording images. These may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. Staff should be aware of the potential for these aspects of teaching to be misused for pornographic or 'grooming' purposes. Careful consideration should be given when they involve young or vulnerable pupils who may be unable to question why or how the activities are taking place.

Good Practice

It is recommended that when using a photograph, the following guidance should be followed:

- If the photograph is used, avoid naming the pupil.
- If the pupil is named, avoid using their photograph.
- Schools should establish whether the image(s) will be retained for further use. Images should be securely stored and used only by those authorised to do so. Photographs can be stored electronically but should be in a secure area.
- Staff should remain sensitive to any children who appear uncomfortable and should recognise the potential for misinterpretation. Avoid taking images in one to one situations.
- Ensure all children are appropriately dressed.
- Avoid images that show a single child with no surrounding context of what they are learning or doing – a group of three or four children are more likely to show the activity to better effect. Use photographs that represent the diversity of the young people participating. Remember to include images of children from different communities in your communications whenever possible, and to use positive images of disabled children. This will ensure that your photographs are inclusive of the whole community and comply with the Disability Discrimination legislation.
- Do not use images that are likely to cause distress, upset or embarrassment.
- Photographs should not be used after a child, or member of staff appearing in them, has left the school.
- Be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded.
- Ensure that a senior member of staff is aware that the school's photography/image equipment is being used and for what purpose.
- Staff should not use their personal photographic/video equipment, nor take images of children and young people using personal mobile telephones.

- Staff should ensure that all images are available for scrutiny and be able to justify images of children in their possession.
- Report any concerns relating to any inappropriate or intrusive photography to the Head Teacher/Manager.
- Accidental/Non-accidental injuries - it is not appropriate to take photographs of a pupil's injuries, as it may cause distress and humiliation. If appropriate seek medical help and in the case of a suspected non-accidental injury contact Social Care as soon as possible.
- School web-sites should avoid using personal details or full names of any child or adult in a photograph, although first names can be used in some circumstances. Also avoid giving personal e-mail, postal addresses, telephone or fax number details.

Parental Permission

- As previously mentioned use of images of children require the consent of the parent/carer. If a parent fails to return a consent form, do not assume that consent is given.
- When a parent does not agree to their child being photographed, the Head Teacher/Manager must inform staff and make every effort to comply sensitively. For example, if a child whose parents have refused permission for photography is involved with a sports event, eg a football match, it may not be appropriate to photograph the whole team. Careful liaison with parents is therefore essential. With discussion it may be possible to agree other options. The parent may accept a team photograph if names are not published or they may be prepared to relent if it affects the whole team.
- When photographic images are transmitted or shared beyond the establishment, eg television broadcasts, images on intranet sites, specific permission should be sought.

Teacher Training and Portfolios

During teacher training and with newly qualified staff, colleagues may need to compile portfolios with photographs of children during lessons. Staff should act responsibly in compiling these images. A member of the senior management team may wish to oversee the compiled images as part of the management process and consider their appropriateness.

Children Photographing Each Other

This practice can occur extensively during offsite activities particularly during residential activities, and for most children it will be the norm to want to take photographs to record the trip or event. Staff should discuss a code of conduct regarding the taking of photographs with the children before the trip. Nevertheless, there may be incidents where children take inappropriate photographs, including showing friends and other children inappropriately dressed. Staff should endeavour to discourage this practice, but ultimately parents are responsible for monitoring their child's use of cameras and subsequent use of the images involved.

Mobile Telephones

Mobile telephones which contain cameras should not be used in changing rooms, toilets, etc.

Use of Internet/intranet Sites

Many establishments will have an internet/intranet facility. The site manager should know good practice and ensure that the establishment only uses appropriate images that follow this guidance. For example, if a child has successfully completed a gymnastics award, it would be appropriate to show the child in a tracksuit rather than a leotard.

Displays in Schools

- Still photographs shown on displays and video clips available during open/parents' evenings should depict children in an appropriate way. They should not display images of children in inappropriate or revealing clothing.
- Parents Evening, Concerts, Presentations
- Ensure and make clear to parent(s)/carer(s) in a letter that photography/video recording only takes place in designated areas. For example, in the main school hall where the assembly or school performance is taking place, and not in 'backstage' areas or school classrooms.
- Encourage parents/carers with video cameras to sit towards the back of the room during assemblies/performances to prevent obscuring other people's view.
- Research the possibility of creating a school video of the event giving parents/carers the option to purchase a copy of the school video. For schools that do not have the right equipment to undertake this, an approach could be made to another school who might agree to loan the necessary equipment.
- A set of photographs could be taken by the school and orders taken for copies. This is made easier where a school has a digital camera.

Newspapers

Children and young people are usually proud and delighted to see themselves in the paper either through an individual success or as part of a team. It is though not acceptable to invite a newspaper to take photographs and then refuse to provide names. Newspapers are unlikely to print anonymous photographs. When an establishment invites a newspaper to take photographs of an event it would be good practice to discuss the requirements with the newspaper first and also to obtain the views/permission of parents/carers.