Growing Ambitious Minds

BOYTON
PRIMARY SCHOOL

Boyton Primary School
Online Safety Policy

September 2024

At Boyton Primary School, we are highly committed to ensuring that our children are provided with a safe, secure and supportive environment in which to learn. We respect and value all children and all staff understand their role in ensuring that all children, regardless of age, disability gender, race, religion or belief, sex or sexual orientation, are protected from all types of harm. We recognise our responsibility to effectively safeguard and promote the welfare of all who access our school. This policy, is to be applied in conjunction with child protection policy, which adheres to the guidance set out within KCSIE 2024. In addition, it relates closely to our behaviour and relationships policy which promotes the welfare of our pupils by protecting them from physical, sexual or emotional abuse, neglect and bullying.

Contents:

1. The purpose of this policy:

At Boyton Primary School, we recognise that the online world has become an integral part of everyday life and while it provides users with many positive opportunities, it can also present risks and challenges. We believe that children, young people and adults within our school should be able to use the internet for education and personal development but we have a duty to ensure that safeguards are put in place to protect them from potential harm when using devices and accessing online opportunities. We have a responsibility to educate our children in how to use the internet and related devices safely, respectfully and responsibility and where they can go to access help if they feel unsafe while online or are worried about the safety of others. We recognise that working in partnership with children, young people, their parents, carers and other agencies is essential in promoting our children's welfare and the development of a responsible approach to online safety.

At Boyton Primary School, we will ensure that:

- The safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- All staff and volunteers are provided with this policy and understand their role when promoting online safety, working safely and responsibly with the internet and other communication devices and the procedures involved in reporting online safety concerns.
- We operate in line with our policy and within the law in terms of how we use online devices.

This policy applies to all members of the Boyton Primary School community (including staff, pupils, students, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of Boyton Primary School.

2. Reporting E-Safety Concerns

Any E-Safety concerns that involve safe guarding or child protection issues are dealt with quickly and sensitively using our safe guarding concerns escalation policy. Concerns identified are reported to the Designated Safe Guarding Lead (DSL) using 'My Concerns'. This policy should be read alongside our Safe Guarding Policy and the correct procedures for reporting child protection concerns and disclosures.

Is it important that incidents are dealt with as soon as possible, in a proportionate manner and that members of the school community involved in the incident are kept updated and know that incidents have been dealt with.

Each incident will be managed on a a case by case basis. In the events of sanctions needing to be applied these are outlined below (this is an indicative not exhaustive list)

For Pupils consequences can include:

- Refer to class teacher
- Refer to Head of school
- Refer to IT support staff for action
- Inform parents/carers
- Removal of internet/access rights
- Where warranted, exclusion

For staff consequences can include:

- Refer to Head of school
- Refer to Governors
- Refer to IT support staff for action
- Warning
- Disciplinary action
- Where warranted, suspension pending investigation

Support is sought from other agencies as needed e.g. the local authority, UK Safer Internet Centre helpline, and MARU where an immediate safeguarding concern is evident.

Parents/carers are specifically informed of online incidents involving young people for whom they are responsible.

If staff or pupils receive online communication that is illegal or of particular concern or there is any suspected online illegal activity taking place, the school will contact the police and related agencies.

Areas of online safety that are of risk to children include, but are not limited to:

Content:

- Exposure to inappropriate content (e.g. online pornography, inappropriate or disturbing images, exposure to violence and racist language/influences from ignoring age ratings on games, substance abuse)
- Inappropriate lifestyle websites (e.g. pro-anorexia/self-harm/suicide sites)
- Hate sites and exposure to radicalisation
- Authenticity and accuracy of online content
- Ignoring age restrictions for accessing social media

Contact:

- Grooming
- All forms of cyber-bullying
- Identity theft, hacking profiles (e.g. Instagram, Facebook) and sharing passwords

Conduct:

- Privacy issues (e.g. disclosing personal, identifying information)
- Digital footprint and online reputation
- Health and wellbeing (e.g. amount of time spent on devices, the internet or gaming)

- Sexting or SGII (sending and receiving personally intimate images/self-generated indecent images) or sending inappropriate or indecent images of others
- Copyright

Response to incidents that occur outside of school
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site. This is pertinent to incidents of cyberbullying or other E-Safety incidents that pose a risk to the welfare of pupils, that take place outside of the school but is linked to membership of the school. Parents and carers will be informed if such incidents of inappropriate E-Safety behaviour take place out of school.

3. E-Safety Curriculum

The aim of our E-Safety curriculum is to provide our children with the skills and knowledge to use the internet, social media and mobile phones and devices safely and securely while showing respect for others. We have a clear, progressive E-Safety education programme as part of our Computing Curriculum and PSHE Curriculum. This ensures that we cover content about a range of skills and behaviours appropriate to pupil's age and experience. We use the 'SMART' rules to visually represent some of the key rules for how to stay safe online. Through this we teach;

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and Security
- Copyright and Ownership

Alongside sessions dedicated to online safety, we aim to embed internet safety issues in all aspects of the curriculum and other school activities. The SMART rules poster is displayed in every classroom and referred to frequently. Online safety is sensitively approached in the EYFS in developmentally appropriate contexts. It has links to the PSED (Personal, Social and Emotional Development) areas of the EYFS curriculum. All teaching staff supervise and carefully support children when engaging in learning activities involving online technologies.

3.1 Online Safety - taught through the Teach Computing curriculum

In addition to our PSHE curriculum, online safety is threaded through the Teach Computing curriculum.

4. Managing the ICT infrastructure

4.1- Internet access, security (virus protection) and filtering

The security of our information systems are regularly reviewed and updated. Our designated IT technician manages and maintains our IT systems. He ensures that our security systems and virus protection are effective and up-to-date. Safe search engines are enabled to ensure that users of the school's IT systems are given maximum protection from accessing potentially harmful material. The IT technician works remotely and on site to ensure that our systems and devices are working effectively and securely for all staff and pupils.

We ensure that user names, logins, email accounts and passwords are used effectively to promote the safety of all users of the school IT systems. Staff are expected to log off or lock computers when leaving for sustained periods and leaving at the end of the day. We examine and assess any social media platforms and new technologies before they are used within the school.

4.2- Use of digital images and videos on school website and social media page

We gain parental/carer consent for use of digital photographs or videos involving their child as part of the data collection form completed when the pupil joins the school. Staff must be vigilant with regard to parental consent provided for uploading children's images and names onto the school website and social media pages and only for the purposes for which consent has been given. Class consents are provided to class teachers and are available on the secure, staff shared area.

We do not identify pupils in online photographic materials or include the full names of pupils alongside photos or videos.

4.3- Staff use of personal mobile phones, mobile devices, social media and email

This is covered in our staff code of conduct.

School staff's social media profiles should not be available to pupils. If they have a personal profile on social media sites, they should avoid using their full name where possible, as pupils may be able to find them. Staff should consider using a first and middle name instead, and set public profiles to private.

Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils' or parents' social media profiles.

Staff will ensure that they do not post any images online that identify children who are pupils at the school without their consent.

Staff will not use technology in school to view material that is illegal, inappropriate or likely to be deemed offensive. This includes, but is not limited to, sending obscene emails, gambling and

viewing pornography or other inappropriate content.
Staff will not use personal mobile phones and laptops, or school equipment for personal use, in school hours or in front of pupils. They should also not use personal mobile phones or cameras to take pictures of pupils. Where this is unavoidable (e.g. where learning needs to be recorded quickly and no other device available), images will be immediately deleted and the staff member will inform SLT to confirm this has happened. Where private phone calls are needed to be taken, staff will use the Co-head office or other office and will remain out of sight of children.
We have the right to monitor emails and internet use on the school IT system.

Staff are provided with an email account for their professional use and understand that personal emails should be managed through a separate account. Staff are mindful and vigilant of possible scams, phishing and virus attachments when opening emails. Concerns can be reported to the GDPR officer who is also the lead on cyber security.

4.4- Students use of personal devices and email

We do not allow pupils to bring mobile phones into school. However, if there are extenuating circumstances that mean it is necessary for a child to bring a mobile phone to school for their own safety, parental permission must be obtained and the phone must be turned off and placed securely in the office/teachers desk upon arrival at school until the end of the day. If pupils breach this, the mobile phone will be confiscated and held securely in the office until the end of the day and parents will be informed.

Students are introduced to email through their computing curriculum. As part of these lessons, children are taught how to compose respectful and responsible emails, awareness of possible risks to opening attachments and links from unknown senders and warning signs to look out for, to not respond to malicious or threatening emails and that they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, worried or is bullying in nature.

4.5- Safety of staff and student personal information

We ensure that personal information about the adults who work at and children who attend Boyton Primary School is held securely and shared only as appropriate.
Egress system is used to transfer sensitive or confidential material via email all correspondence is encrypted and password protected.

4.6- School Website

Staff members have individual logins for the school website in order to upload photos, videos and written content. Photographs and videos published on the website do not have the full names of children attached. Our school website has a designated lead who ensures DFE compliance and accurate, current and pertinent information is available. The security of the site is monitored by a professional 3rd party.

4.7- Staff laptops

All staff are trained and given guidance on how to maintain cyber security on school laptops and sign a user agreement on receipt on a school based device. The school IT technician can remotely access to check and monitor appropriate staff usage.

All usage surrounding staff laptops is to be done in line with the school code of conduct. Staff must not share their passwords with family members.

5. Useful websites for Online Safety information and support

https://saferinternet.org.uk/

https://www.gov.uk/government/organisations/uk-council-for-internet-safety

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf

https://static.purplemash.com/mashcontent/applications/purplemash_in_england/PM_Education_for_a_connected_world/Education%20for%20a%20Connected%20World.pdf