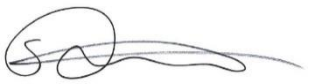
WETHERBY
PREPARATORY SCHOOL

Alpha Plus group
the Gold Standard in education

Wetherby Preparatory School
Bryanston Square
London W1H 2EA

020 7535 3520

Online Safety Policy

Policy reviewed by:	Stephen Blundell
Review date:	September 2021
Submission date:	September 2021
Policy actioned from:	September 2021 – August 2022
Next review date:	June 2022
Reviewer's signature:	
Headmaster's signature:	

Circulation: This policy is addressed to all members of staff and volunteers and is available to parents on request. It applies wherever staff or volunteers are working with the boys.

Please note: 'School' refers to Wetherby Preparatory School and 'parents' refers to parents, guardians and carers.

Contents

1 Aims

1.1 This is the online safety policy of Wetherby Preparatory School.

1.2 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

1.2.1 protects the whole School community from illegal, inappropriate and harmful content or contact;
1.2.2 educates the whole School community about their access to and use of technology;
1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate; and
1.2.4 promotes a whole school culture of safety, equality and protection.

1.3 This policy forms part of a whole school approach to promoting child safeguarding and wellbeing, which seeks to ensure that the best interests of pupils underpins and is at the heart of all decisions, systems, processes and policies.

1.4 Online safety is a running and interrelated theme throughout many of the School's policies and procedures (including its child protection and safeguarding policy and procedures) and careful consideration has been given to ensure that it is also reflected in the School's curriculum, teacher training and any parental engagement, as well as the role and responsibility of the School's Designated Safeguarding Lead.

2 Scope and application

2.1 This policy applies to the whole School.

2.2 This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

3 Regulatory framework

3.1 This policy has been prepared to meet the School's responsibilities under:

3.1.1 Education (Independent School Standards) Regulations 2014;
3.1.2 Education and Skills Act 2008;
3.1.3 Children Act 1989;
3.1.4 Childcare Act 2006;
3.1.5 Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**); and
3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2021) (**KCSIE**);
3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfDCMS and UKCIS, December 2020);
3.2.4 Revised Prevent duty guidance: for England and Wales (Home Office, April 2021);
3.2.5 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, February 2021);
3.2.6 Sexual violence and sexual harassment between children in schools and colleges (DfE, September 2021);
3.2.7 Searching, screening and confiscation: advice for schools (DfE, January 2018);
3.2.8 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019);
3.2.9 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, June 2019);
3.2.10 Teaching online safety in schools (DfE, June 2019);
3.2.11 Harmful online challenges and online hoaxes (DfE, February 2021);
3.2.12 Online safety guidance if you own or manage an online platform (DfDCMS, June 2021);
3.2.13 A business guide for protecting children on your online platform (DfDCMS, June 2021);
3.2.14 Online safety audit tool (UKCIS, August 2020).

3.3 The following School policies, procedures and resource materials are relevant to this policy:

3.3.1 acceptable use policy for pupils;
3.3.2 staff IT acceptable use policy and social media policies;
3.3.3 child protection and safeguarding policy and procedures, including guidance on peer on peer abuse;
3.3.4 anti-bullying policy;
3.3.5 risk assessment policy;
3.3.6 staff code of conduct and whistleblowing policies;
3.3.7 data protection policy;
3.3.8 use of mobile phones and electronic devices;
3.3.9 behaviour, discipline and exclusion policy;
3.3.10 relationships and sex education policy.

4 Publication and availability

4.1 This policy is published on Wetherby Preparatory School's policy portal.

4.2 This policy is available in hard copy on request from the School Office. It can be made available in large print or other accessible format if required.

5 Definitions

5.1 In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**).

6 Responsibility statement and allocation of tasks

6.1 Alpha Plus Group has overall responsibility for all matters which are the subject of this policy. It ensures that all those with leadership and management responsibilities at the School actively promote the well-being of pupils.

6.2 The Designated Safeguarding Lead (**DSL**; see contents page for contact details) has primary responsibility for the implementation and maintenance of this policy at school level. The policy is updated as required and formally reviewed on an annual basis.

6.3 Online safety incidents are reviewed as part of an ongoing cycle of governance visits, and as part of an annual safeguarding review conducted by the Nominated Safeguarding Governor and DSL.

6.4 Taking into account the multi-dimensional aspects of online safety, specific responsibilities are assigned to specific individuals based on their skills and experience, as set out below:

Aspect of Online Safety	Designated Person[1]
ICT Coordinator	Dean Bayes
On-Site Engineer[2]	Lance Coleman
Curriculum – ICT	Dean Bayes
Curriculum – PSHE	Chloe Hood
Staff Training and CPD	Stephen Blundell
Development of Parental Awareness	Nick Baker

7 Role of staff and parents

7.1 Headmaster and Senior Leadership Team

7.1.1 The Headmaster has overall executive responsibility for the safety and welfare of members of the School community.

7.1.2 The DSL is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the DSL includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's child protection and safeguarding policy and procedures.

7.1.3 The DSL will work with the School's On-Site Engineer and ICT Coordinator (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

7.1.4 The DSL will monitor the School's online safety incident log.

7.1.5 The DSL will regularly run reports using the filtering software to identify risk alerts and concerns.

7.1.6 The DSL will regularly update other members of the School's Senior Leadership Team on the operation of the School's safeguarding arrangements, including online safety practices.

[1] A person may cover more than one aspect if they have the appropriate experience and skills-set.

[2] The on-site engineer must sign the annual affirmation statement as required by the Code of Ethical and Professional Conduct (available on the Portal).

7.2 **Alpha Plus Group Director of IT and IT Team**

7.2.1 Alpha Plus Group's Director of IT, together with his team of On-Site Engineers, is responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network. This includes responsibility for ensuring that:

(a) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;
(b) the user may only use the School's technology if they are properly authenticated and authorised;
(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;
(d) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;
(e) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and
(f) monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

7.2.2 Whilst the above responsibilities sit with the Alpha Plus Group Director of IT and are administered by the School's On-Site Engineer, it is essential that a member of staff is nominated as ICT Coordinator and is assigned responsibility for monitoring the effective delivery of technology services on behalf of all school/college users, and for reporting problems where necessary. The ICT Co-ordinator may also be responsible for the ICT curriculum, but it is important that these two responsibilities are clearly understood as separate functions.

7.2.3 The ICT Coordinator will report regularly to the Senior Leadership Team on the operation of the School's technology. If the ICT Coordinator has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the DSL and Alpha Plus Group's Head Office IT team.

7.2.4 The ICT Coordinator is responsible for bringing any matters of safeguarding concern to the attention of the DSL in accordance with the School's child protection and safeguarding policy and procedures.

7.3 **All staff**

7.3.1 All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

7.3.2 Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

7.3.3 All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to-face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.

7.3.4 Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school. Examples of such abuse can include:

(a) the sending of abusive, harassing and misogynistic messages;

(b) the consensual and non-consensual sharing of indecent images and videos (especially around group chats), which is sometimes known as sexting or youth produced sexual imagery;

(c) the sharing of abusive images and pornography to those who do not wish to receive such content;

(d) cyberbullying.

7.3.5 Staff are also aware that many other forms of abuse may include an online element. For instance, there may be an online element which:

(a) facilitates, threatens and/or encourages physical abuse;

(b) facilitates, threatens and/or encourages sexual violence; or

(c) is used as part of initiation/hazing type violence and rituals.

7.3.6 It is important that staff recognise the indicators and signs of peer on peer abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of peer on peer abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.

7.3.7 It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "*just banter*", "*just having a laugh*", "*part of growing up*" or "*boys being boys*" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. The School has a **zero tolerance approach** towards peer on peer abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's behaviour and discipline policy and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures.

7.3.8 Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's child protection and safeguarding policy and procedures. If staff have any concerns regarding peer on peer abuse or if they are unsure as to how to proceed in relation to a particular incident, they should **always speak to the DSL in all cases (see contact details on cover page).**

7.3.9 Staff authorised by the [Head/Principal] have the right to search for, examine and confiscate any device where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. This will be done in accordance with the Department for Education's guidance: Searching, screening and confiscation (2018). Inappropriate usage will be dealt with consistent with the School's policy on behaviour and discipline. Following an examination of an electronic device, the member of staff has the right to erase any data or files, if they think there is a good reason to do so. However, care should be taken

not to delete material that might be required in a potential criminal investigation. If a member of staff has reasonable grounds to suspect that a device contains evidence in relation to an offence, they must alert the Headmaster and, where there are safeguarding concerns, the DSL. The device should then be given to police as soon as is reasonably practicable.

Although the maintenance of technological controls (see section below) such as internet filtering, and data and network security are the responsibility of the Alpha Plus Group Director of IT and administered by the On-Site Engineer, **it is essential that a member of school staff is nominated as ICT Coordinator and is assigned responsibility for monitoring the effective delivery of these services on behalf of all school users, and for reporting problems where necessary.** The ICT Coordinator may well be also responsible for the ICT curriculum, but it is important that these two responsibilities are clearly understood as separate functions.

Training and CPD

Those responsible for E-safety will keep up to date on current E-safety issues and guidance issued by the Government and by organisations such as their Local Authority, CEOP (Child Exploitation and Online Protection) and Childnet International.

Consistent with our *Safeguarding policy*, all staff:

- receive information and training on E-safety, both at induction, and at regular intervals thereafter (minimum annually),

- have a duty to be alert to E-safety, and to share any concerns with the DSL (and others as appropriate in the context).

Understanding the types of E-safety risk

Risks commonly associated with new media and technology are broad. In most cases the risks are not intrinsically caused by technology, but technology may increase the ease and likelihood of occurrence, and increase the scope of potential harm. Risks include:

1. Predatory behaviours such as grooming, abuse or radicalisation,
2. The corruption of young minds through the normalisation of disrespectful, or anti-social language and behaviour through exposure to age-inappropriate content[3], especially: violence, pornography, racism, sexism, gambling, advertising, etc.
3. Extensions of 'off-line' peer-behavioural risks, e.g. peer on peer abuse, cyber-bullying, 'trolling',
4. The misplaced perception that aggressive, offensive and inconsiderate on-line language or behaviour is somehow less damaging and more acceptable than their equivalents off-line or face to face.
5. The degradation of educational and maturing processes arising from a child's misplaced judgement of the accuracy, reliability or contextual propriety of online content,

[3] Online games designed for adults are often cited as one of the principle causes of concern for several of these risks. This may be as much from the highly aggressive and verbally abusive behaviours they elicit as from the be-friending of pseudonymous strangers or from exposure to violent and sexual content. **Extensive exposure to such games may be considered evidence of child neglect, which may, in certain circumstances, lead schools/colleges to consider reporting parents to social services.**

6. Breaking laws, e.g. sexting, copyright infringement, data protection/privacy breaches,
7. The lasting damage to self-esteem and to reputation which children may incur (to themselves or to others, thoughtlessly or maliciously) by distributing or publishing confidential, insensitive, offensive or otherwise inappropriate content,
8. Exposure to fraud, hacking or identity-theft through insufficient security of passwords and personal details,
9. The use of new media and technology in distracting or addictive ways.

In order to develop age-appropriate responses to this wide range of risks, we categorise them, along with related learning objectives, as follows (adapted from Tanya Byron's '3 C's of E-safety'):

Risk category	Commercial	Aggressive	Sexual	Values
Content Child is observer / consumer	Understand and develop resilience to advertising, spam, sponsorships and demands for personal information	Develop resilience to violent / hateful content and know how to cope and to deal with it	Avoid / develop resilience to pornographic or unwelcome sexual content	Develop critical evaluation skills to Identify bias, prejudice, misleading and manipulative information and advice
Contact Child is participant	Awareness of tracking, harvesting and the protection of personal information	Develop resilience to being bullied or harassed, and know what actions to take	Understand the implications of interacting with strangers and being groomed	Develop resilience to the risk of compulsive/addictive online behaviour, and to unwelcome persuasions
Conduct Child is instigator / perpetrator	Clear guidance on illegal downloading, copying, plagiarising, hacking, gambling, fraud, identity theft and the consequences	Clear guidance on bullying, harassment or 'trolling' of others and understand the consequences	Clear guidance on creating and uploading inappropriate material and understand the consequences	Clear guidance on the value of personal integrity, respect, data security, confidentiality, and the consequences of publishing inappropriate, false or misleading information or advice

Key principles and controls

We take E-safety very seriously. In addition to all the general safeguarding principles and controls included within our *Safeguarding policy*, the over-arching principle with E-safety is the need to educate the boys about the risks and benefits of using new media and technology, and to help them to operate safely, legally, productively, thoughtfully and considerately in the digital world. This includes the development of independent thinking and critical evaluation skills to help determine the reliability, accuracy and integrity of on-line content.

E-safety is incorporated into the curriculum, not only within ICT and PSHE lessons, but wherever and whenever it makes sense to reinforce concepts at an age-appropriate level. This includes assemblies, guest speakers, and parent information events. We believe that the internet and the constantly evolving technologies and devices to which the boys have access can be tools that enrich their lives. We therefore teach them to view technology and new media positively whilst simultaneously protecting themselves.

Technological controls

In addition to the educational measures to promote E-safety within the curriculum, we maintain specific controls which enable us to establish a secure data and communications environment and to monitor the boys' digital activity within the boundaries of the school. Foremost amongst these are:

a) Boys to whom we provide bespoke[4] access to ICT resources are asked to agree in writing to a set of rules for the acceptable use of such resources (see *ICT Usage policy*).

b) Our password-controlled network maintains individual security, confidentiality and accountability for activity on the network. Impero software ensures that computer activity can be monitored in real time. Lightspeed is used to monitor search history and pupil use at school and at home.

c) We use well-established and frequently updated filtering software to prevent access to content deemed to be potentially harmful, and which records attempts to access such potentially harmful content. If staff or boys discover unsuitable sites, the URL (web address) must be reported to the ICT Coordinator. Any member of the school community should report a website which causes them concern to the ICT Coordinator who will immediately refer this to the on-site engineer who will arrange for that site to be blocked, always taking care to consider that potential 'over-blocking' does not lead to unreasonable restrictions in online learning.

The scope of the technological controls mentioned above extends across all our network of computers and internet-enabled devices, and across any Wi-Fi access which the school operates.

Whilst these filtering controls can similarly apply to mobile phones which use the school Wi-Fi, we cannot (legally or technically) monitor private phone activity, e.g. texting, or applications or internet content which are accessed via 3G, 4G and 5G signals. For this reason we operate a strict policy on the use of mobile phones (see separate policy document).

[4] E.g. email accounts; network ID's and accounts; unsupervised browsing.

Our staff are authorised to search for[1] and to confiscate any device. They can also search the device and (if appropriate) delete content if they consider that it has been, or could be used to cause harm, to disrupt teaching or break the school rules. Inappropriate usage will be dealt with consistent with our policies on discipline, behaviour, sanctions and exclusions. If a member of staff has reasonable grounds to suspect that a device contains evidence in relation to an offence, they must give it to police as soon as is reasonably practicable. Any evidence of an offence or material that contains a pornographic image of a child should not be deleted prior to giving the device to the police.

The School ICT Coordinator has specific responsibility for monitoring the effectiveness of the technological controls section of this policy, under the direction of the Alpha Plus Group Director of IT.

Parental responsibilities and off-site E-safety

Given that boys' engagement with the digital world extends well beyond the school premises, we expect parents to remain alert to their son's activities and behaviour. We recognise that this is a broad and open-ended task which many parents find challenging. We therefore direct parents towards on-line resources which can help parents to take preventative action which will promote E-safety, and help them to identify risk-indicators of potentially problematic behaviour. We host workshops for parents to support strategies for staying safe online and we encourage parents to attend these where possible.

Regarding the responsibility of schools to deal with E-safety incidents which occur 'off-site', the Education and Inspections Act 2006 and the Education Act 2011 empower the school, to such extent as is reasonable, to:

- regulate the behaviour of children when they are off the school site where an E-safety incident is linked to the school
- impose disciplinary penalties for inappropriate behaviour
- search for and confiscate electronic devices, and search their contents, and where appropriate delete content

Reporting of E-safety incidents

An E-safety incident[5], which includes the discovery of a specific or heightened risk, must be reported as soon as possible. If it in any way touches on child safeguarding issues, then it must be reported immediately to the DSL, consistent with the *Safeguarding policy*. Similarly, if it involves cyber-bullying, then the *Anti-Bullying policy* must be followed.

If it relates to technological controls (as described above), or to a breach of the *ICT Usage policy*, then it must be reported to the ICT Coordinator. Other members of staff and management should be informed as appropriate in the circumstances.

A log of E-safety incidents should be maintained. The reporting of E-safety Incidents should include the following data:

---

[1] If in doubt, staff should consult their Headmaster and the Department for Education guidance: ***Searching, screening and confiscation*** (2018).

[5] This may be understood as something of a serious nature which requires disclosure and remedial action.

- Name of person reporting the incident
- Date and time of incident
- Date reported
- Names of people involved
- Location and device details
- Details of incident, including evidence where possible
- Clarification of the risk or breach – e.g. does it relate to safeguarding, bullying, inappropriate content, sexting, data protection, copyright infringement…etc.? Use the 3 C's categorisation as described earlier in this policy.
- Initial action taken and current status

Once investigated, a record of the resolution of the incident, and actions taken as a result, must be maintained. Such records should be readily available for inspection during governance visits. Data in the E-safety log will be processed in line with Alpha Plus Group's Privacy Notice, which is available on request or can be accessed via the Group's public portal.