Wetherby Kensington
4 Wetherby Gardens
London
SW5 0JN

# E-Safety Policy

**Policy reviewed by:** Lauren Vallely and Helen Milnes

**Review date:** July 2021

**Submission:** July 2021

**Policy actioned from:** September 2021 – August 2022

**Next review date:** July 2022

**Reviewer's Signature:** Lauren Vallely Helen Milnes

**Head Teacher's Signature:** Helen Milnes

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

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

# E-safety Policy

## Contents

- Scope and definition
- Responsibilities
- Training and CPD
- Understanding the types of E-safety risk
- Key principles and controls
- Technological controls
- Parental responsibilities and off-site E-safety
- Reporting of E-safety incidents

## Appendices

- 1 - E-Safety Incident Log form
- 2 - E-Safety Incident Flowchart
- 3 - E-safety During a Period of School Closure
- 4 - Example email to parents about security settings on their devices

## Scope and definition

This policy is part of our strategy for safeguarding children within our care. It complies with *Keeping Children Safe in Education (KCSIE) September 2021.*

E-safety is a broad term which we use to refer to the safeguarding of children in relation to the risks arising from ever-evolving new media and technologies such as: the internet, mobile phones, tablets, computers, gaming devices, instant messaging, social media, collaboration tools, personal publishing, and 'apps' in general.

The responsible use of technology is a multi-dimensional, social and behavioural issue. Although the generic term 'E-safety' implies a response to some specific risks (as described below), we do not regard it as a stand-alone topic. It is embedded within our educational processes and consequently we take a holistic approach to keeping children safe. This policy should therefore be read in conjunction with our other policies, notably:

- Safeguarding
- Anti-Bullying
- Learning for Life (PSHE)
- Use of Mobile Phones and other Electronic Devices
- Images
- ICT Usage
- Social Media

## Responsibilities

The Designated Safeguarding Lead (DSL) has primary responsibility for the implementation and maintenance of this policy. Taking into account the multi-dimensional aspects of E-safety, it is essential that specific responsibilities are also clearly assigned to specific individuals based on their skills and experience.

| Aspect of E-safety | Designated person[1] |
|---|---|
| Digital Literacy Leaders | Helen Milnes and Jessica Preece |
| On-site Engineer[2] | DSA provided by Alpha Plus |
| Curriculum - ICT | Emily Rubbert |
| Curriculum - PSHE | Lauren Vallely |
| Staff Training & CPD | Helen Milnes |
| Development of Parental Awareness | Helen Milnes, Jessica Preece and Lauren Vallely |

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

[2] Even if not directly employed by Alpha Plus, the on-site engineer must sign the annual affirmation statement as required by the Code of Ethical & Professional Conduct (available on the Portal).

Clarification of the relationship between the Digital Literacy Leader and the On-Site Engineer

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 Digital Literacy Leader 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 Digital Literacy Leader 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 normalization 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. 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.
6. Breaking laws, e.g. sexting, copyright infringement, data protection/privacy breaches.

[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.**

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**<br>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**<br>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**<br>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 children 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 Learning for Life (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 children 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 children's digital activity within the boundaries of the school. Foremost amongst these are:

a) Children 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.

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 children discover unsuitable sites, the URL (web address) must be reported to the ICT Leader. Any member of the school community should report a website which causes them concern to the ICT Leader who will immediately refer this to the on-site engineer who will arrange for that site to be blocked.

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 and 4G signals. For this reason we operate a strict policy on the use of mobile phones (see Mobile Phones and Electronic Devices Policy).

Our staff are authorised to search for[5] 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 the 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 Digital Literacy Leader 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 children's engagement with the digital world extends well beyond the school premises, we expect parents to remain alert to their children'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 expect parents to attend at least one of these annually.

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

[5] If in doubt, staff should consult their Head/Principal and the Department for Education guidance: ***Searching, screening and confiscation*** (February 2014).

Regarding the responsibility of schools/colleges to deal with E-safety incidents which occur 'off-site', the Education and Inspections Act 2006 and the Education Act 2011 empower the school/college, 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/college

- 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[6], 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 Leader.

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:

- 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.

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

## Appendix 1

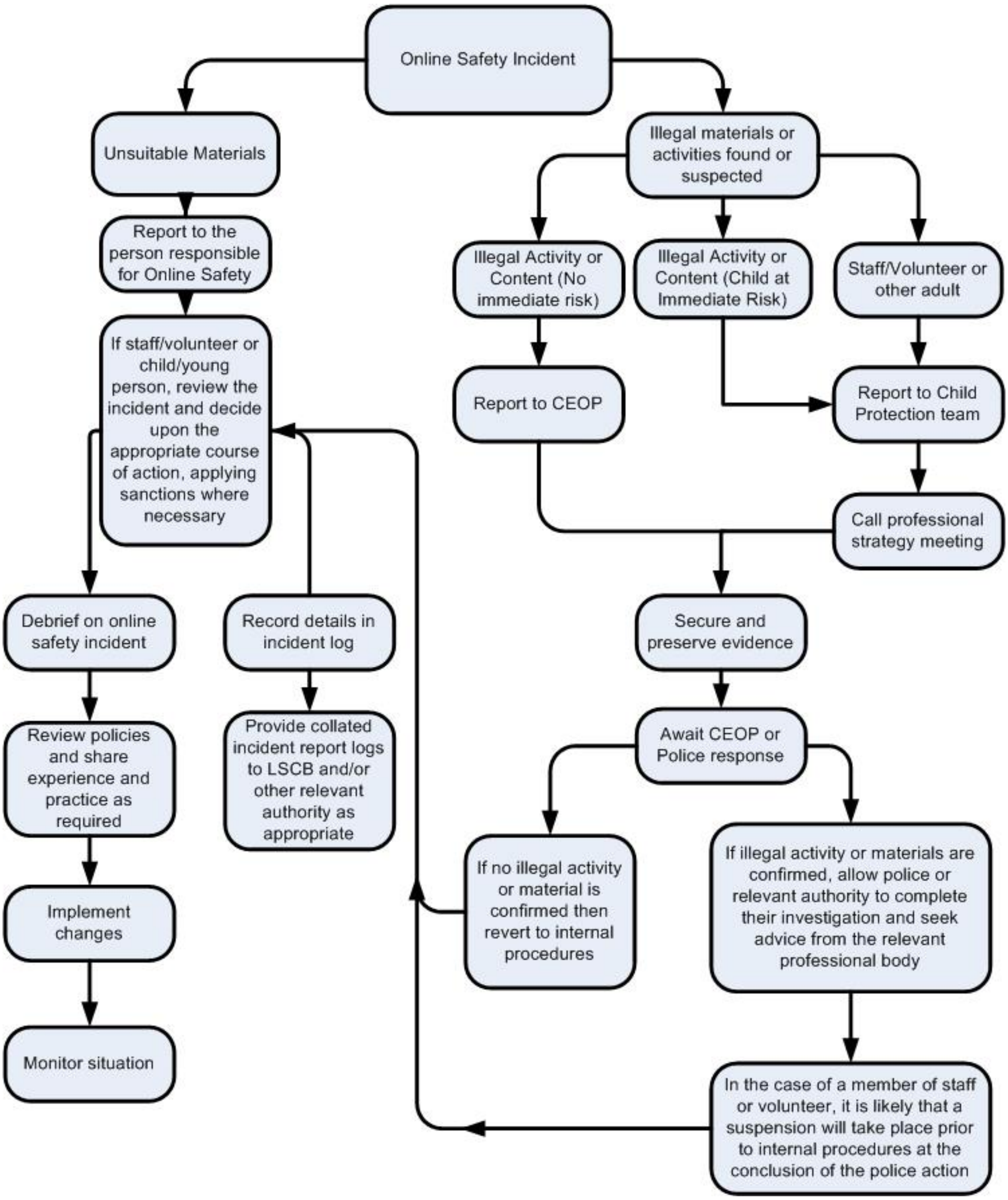
# E-Safety Incident Log Form

| | |
|---|---|
| Name of person reporting incident: | |
| Date and time of incident: | |
| Date incident reported: | |
| Names of people involved: | |
| Location and device details: | |
| Details of incident, including evidence: | |
| Clarification of the risk or breach e.g. does it relate to safeguarding, bullying, inappropriate content, data protection, copyright, infringement, sexting, etc? (Use 3Cs categorisation): | |
| Initial action taken and current status: | |
| Resolution of incident: | |

## Appendix 2

# E-Safety Incident Flowchart

Please report any e-safety issues to either the Headmistress or the Designated Safeguarding Lead.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## Appendix 3

## E-Safety during a period of school closure

During a period of closure, Wetherby Kensington will move to remote learning and Microsoft Teams will be used to deliver live and recorded sessions. The welfare and safety of the boys will remain a priority and the usual safeguarding procedures will be adhered to, as outlined in the school's Safeguarding Policy and KCSIE 2021. This appendix establishes the additional measures that will be taken to ensure an awareness of online safety.

### Online Safety

During a period of closure, e-safety and ICT usage policies will continue to be followed. During remote teaching and learning, Wetherby Kensington will ensure the provision of a safe online environment for boys. Through the use of Microsoft Teams, all personal details and academic resources and files will remain secure and accessible only to those granted access by Alpha Plus. Teachers will remain vigilant when setting assignments and providing resources and continue to check the suitability of all online resources used and recommended. Staff will receive dedicated training on the use of Microsoft Teams and will be supported in the use of Microsoft Teams by the IT Operations Engineer. In the event of this member of staff being unavailable, support will be provided by the Alpha Plus IT department. Parents should ensure that the device used by their son(s) is set up with appropriate web-filtering and parental controls. Parents (or a responsible adult) should remain in the room whilst their son participates in any one to one online lessons and there should be a responsible adult in the house whilst boys participate in group online lessons. It is recommended that the door remains open to the room in which a boy is participating in a lesson.

### One to one meetings and lessons

At times it might be necessary for one to one sessions to take place between teachers and boys, specifically those who already receive one to one support in school. As with all lessons and meetings on Microsoft Teams, these will be recorded. Parents or carers must remain in the room with their son(s) whilst any online one to one session is taking place.

### Recording of lessons

All group lessons, one to one lessons and meetings will be recorded. Recordings will be accessible only to those that attended the session. These recordings will automatically save to the 'chat' and will be accessible only to those who attended the online session. They will not be shared and are taken purely in the interest of safeguarding. Parents and boys are not permitted to record anything school-related in which they participate or which they view on Microsoft Teams and under no circumstances should they share anything outside the school community. Recordings will be kept for at least 21 days and as a maximum, up to one year, to allow time for any concerns to be raised. The recordings will then be deleted.

### Staff

During a period of closure, and the move to remote teaching and learning, staff must adhere to the Remote Learning Staff Code of Conduct. High levels of professionalism and the maintaining of appropriate boundaries will be expected at all times. Staff are expected to dress appropriately at all times and ensure they are well prepared for lessons, with all resources prepared and to hand. Staff are advised to select their location carefully and consider using the 'blurred background' option. All teaching, one to one sessions and meetings must be recorded. Under no circumstances should a teacher share content or images from Microsoft Teams outside the whole school community. Any contact between staff and boys should take place via Microsoft Teams. In exceptional circumstances, a phone call to a family might be necessary. Staff should withhold their personal phone number and should not store contact details of parents on their personal devices. Private tutoring must happen only at the discretion of the Headmistress and should not go ahead without her knowledge. Any concerns about the behaviour of a member of staff should be reported as per Appendix 6 (Concerns and allegations about staff) in the Safeguarding Policy. During a prolonged period of closure, it might be necessary to recruit staff for the following term or academic year. The Alpha Plus Group and its schools and colleges operate 'safer recruitment' procedures as outlined in Alpha Plus Group's recruitment policy and in accordance with Part three of KCSIE (2019). Further details can also be found on page 24 of the Safeguarding Policy.

**Online behaviour**

Whilst participating in remote learning, boys will be expected to behave as an 'Online Wetherby Ambassador' at all times. They should be appropriately dressed and prepared for their lessons. They will be expected to remain in their chosen room for duration of the lesson and follow the behaviour guidelines given by their teachers in regards to their conduct and their use of the microphone. A system of 'strikes' will be implemented by all teachers and staff will have the option to remove boys from lessons in the instance of ongoing disruptive behaviour.

**Reporting concerns**

Staff will remain vigilant and will act immediately if they have a concern regarding the safety or welfare of a child. Staff should continue to follow school procedures and report any concerns via My Concern. In the unlikely event that a member of staff cannot access My Concern from home, they should telephone the DSL. If they cannot reach the DSL on the phone, they should email the DSL, the Headmistress and all members of Senior Leadership Team to ensure that the concern is received. Staff are advised to send information in a password protected file with the details of the concern and communicate the password separately. Staff should ensure they report any concern immediately and without delay.

If parents have any concerns regarding the welfare of a child, they should report this immediately to the Deputy Head (Pastoral), Miss Lauren Vallely, who is the Designated Safeguarding Lead (DSL) or the Deputy DSL, Helen Milnes the Headmistress. Please see page 2 of the school's Safeguarding Policy for contact details for Lauren Vallely and Helen Milnes, and page 4 of the policy for contact details of the Senior Leadership Team.

## Appendix 4

### Email to parents regarding security settings

Dear parents,

When your son is learning remotely, we would like to ensure that your security settings on your devices are as safe as possible. Please click on the following link to learn how to set your device(s) to restricted mode:

https://support.google.com/youtube/answer/

You can also run an ad blocker on Google Chrome. Please click on the following link to access this:

https://chrome.google.com/webstore/

We will also be using www.youtubekids.com which has no ads and is child friendly. As a school we would recommend if you do want to access YouTube for your sons that you use the children's version instead.

Yours sincerely,