



## Online Safety Policy

---

### HILDENGRANGE SCHOOL

Date of adoption of this policy	September 2021
Date of last review of this policy	September 2021
Date for next review of this policy	June 2022
Policy owner	<p><b>Designated Safeguarding Lead (DSL)</b></p> <ul style="list-style-type: none"><li>• <b>Rosemary Jubber</b></li></ul> <p>Email: <a href="mailto:rosemary.jubber@hildengrange.co.uk">rosemary.jubber@hildengrange.co.uk</a></p> <p>Telephone number (term time): 01732 352706</p> <p>Mobile number (term time): 07715207940</p> <p>Holiday contact number: 07715207940</p> <p><b>Deputy Designated Safeguarding Leads (DDSL)</b></p> <ul style="list-style-type: none"><li>• <b>Natalie Brown</b></li></ul> <p>Email: <a href="mailto:natalie.brown@hildengrange.co.uk">natalie.brown@hildengrange.co.uk</a></p> <p>Telephone (term time): 01732 352706</p> <p>Mobile number (term time): 07810541868</p> <p>Holiday contact number: 07810541868</p> <ul style="list-style-type: none"><li>• <b>Sheena Sowerby</b></li></ul> <p>Email: <a href="mailto:sheena.sowerby@hildengrange.co.uk">sheena.sowerby@hildengrange.co.uk</a></p> <p>Telephone (term time): 01732 352706</p> <p>Mobile number (term time): 07957972834</p> <p>Holiday contact number: 07957972834</p> <p><b>Online Safety Officer</b></p> <ul style="list-style-type: none"><li>• <b>Darren Cank</b></li></ul> <p>Email: <a href="mailto:darren.cank@hildengrange.co.uk">darren.cank@hildengrange.co.uk</a></p>



## Contents

1	Aims .....	3
2	Scope and application .....	3
3	Regulatory framework.....	3
4	Publication and availability.....	5
5	Definitions.....	5
6	Responsibility statement and allocation of tasks.....	5
Aspect of online safety .....		5
7	Role of staff and parents .....	6
8	Technological controls.....	9
9	Procedures for dealing with online safety concerns and incidents .....	11
10	Education .....	14
11	Training.....	15
12	Risk assessment .....	18

## 1 **Aims**

- 1.1 This is the online safety policy of HILDEN GRANGE 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 including the Early Years Foundation Stage (**EYFS**).
- 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 Statutory framework for the Early Years Foundation Stage (DfE, September 2021);
  - 3.1.3 Education and Skills Act 2008;
  - 3.1.4 Children Act 1989;
  - 3.1.5 Childcare Act 2006;
  - 3.1.6 Data Protection Act 2018 and UK General Data Protection Regulation (**UK GDPR**); and
  - 3.1.7 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 school rules;
  - 3.3.10 relationships and sex education policy.

#### 4 **Publication and availability**

- 4.1 This policy is published on the School website.
- 4.2 This policy is available in hard copy on request. 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 cover 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:

<b>Aspect of online safety</b>	<b>Designated person</b>
Head of IT	Darren Cank
On-site Engineer <sup>1</sup>	Peter Patience
Curriculum - ICT	Darren Cank
Curriculum - PSHEE	Natalie Brown
Staff Training & CPD	Jason Davie
Development of Parental Awareness	Natalie Brown and Darren Cank

<sup>1</sup> The on-site engineer must sign the annual affirmation statement as required by the Code of Ethical & Professional Conduct (available on the Portal).

## **7 Role of staff and parents**

### **7.1 Head and Senior Leadership Team**

- 7.1.1 The Head 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.

### **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 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 Head and, where there are safeguarding concerns, the DSL. The device should then be given to police as soon as is reasonably practicable.

## 7.4 Parents

- 7.4.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. The School expects parents to promote safe practice when using technology and to:
- (a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;
  - (b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and
  - (c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.



7.4.2 If parents have any concerns or require any information about online safety, they should contact the DSL.

## 8 Technological controls

- 8.1 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.
- 8.2 Children to whom we provide bespoke<sup>2</sup> 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).
- 8.3 Our password-controlled network maintains individual security, confidentiality and accountability for activity on the network. Any pupil or member of staff who has a problem with their user names or passwords must report it to the School's ICT team immediately.
- 8.4 The School uses 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 Coordinator. Any member of the School community should report a website which causes 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.
- 8.5 The use of any device connected to the School's network will be logged and monitored by the ICT team.
- 8.6 The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the ICT team.
- 8.7 **Inappropriate material**
- 8.7.1 The School recognises the importance of ensuring that all pupils are safeguarded from potentially harmful and inappropriate material online.
- 8.7.2 Online safety is a key element of many school policies and procedures and an important part of the role and responsibilities of the DSL. The term 'online safety' encapsulates a wide range of issues but these can be classified into four main areas of risk
- (a) **Content** - being exposed to illegal, inappropriate, inaccurate or harmful content (e.g. pornography, extreme violence, addictive content, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism)<sup>3</sup>;

<sup>2</sup> E.g. email accounts; network ID's and accounts; unsupervised browsing

<sup>3</sup> 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 the School to consider making a report to social services.

- (b) **Contact** - being subjected to harmful online interaction with other users (e.g. peer to peer pressure, bullying, harassment, threats to privacy, commercial advertising and adults posing as children or young adults with the intention to groom and/or exploit them for sexual, criminal, financial or other purposes);
- (c) **Conduct** - a pupil's personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending and receiving explicit images (such as consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, harassment, breaching copyright; and
- (d) **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The school is committed to supporting awareness of these risks in age-appropriate ways and to building resilience and critical thinking skills to enable students to respond appropriately to such risks. See the table below (adapted from Tanya Byron's '3 C's of E-safety') and section 10 for further information about online safety education.

Risk category	Commercial	Aggressive	Sexual	Values
<b>Content</b> 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
<b>Contact</b> 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
<b>Conduct</b> 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

## 8.8 Use of mobile electronic devices and smart technology

- 8.8.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email text messaging and social media sites) when connected to the School's network. Mobile devices and smart technology equipped with a mobile data subscription can, however, provide pupils with unlimited and unrestricted access to the internet. The School is alert to the risks that such access presents, including the risk of pupils sexually harassing their peers using

their mobile or other smart technology; or sharing indecent images consensually or non-consensually; or viewing and/or sharing pornography and other harmful content. Therefore, the School operates a clear mobile usage policy and has mechanisms in place to manage such risks.

- 8.8.2 The School uses the Smoothwall Firewall service as managed both internally by the DSL and on-site engineer as well as externally by Smoothwall themselves regularly updating their service to block access to inappropriate web content. The school Mobile Device Policy states that students must not bring a mobile phone into school unless they walk home alone or are in the upper school in which case the phone is kept in the school office for the duration of the school day. School provided iPads are managed using dataJAR to prevent students from installing applications from the Apple App Store and are also protected by the Smoothwall Firewall as described above. School provided Surface Go devices are managed using Windows Group Policies and are also protected by the Smoothwall Firewall as described above.
- 8.8.3 In no circumstances, a pupil may be given permission to use their own mobile device or other smart technology to connect to the internet using the School's network.
- 8.8.4 The School rules about the use of mobile electronic devices or other smart technology, including access to open / non-School networks, are set out in ICT Usage Policy published September 2021.
- 8.8.5 The use of mobile electronic devices by staff is covered in Staff code of conduct policy, Staff IT acceptable use polices, social media policy, data protection policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.
- 8.8.6 The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use 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.

## 9 Procedures for dealing with online safety concerns and incidents

### 9.1 Concerns/Incidents relating to pupils

- 9.1.1 **Anyone** who has **any** concern about pupils' online safety, the misuse of technology or a particular risk should report it immediately.
  - (a) If a concern or incident in any way touches on child safeguarding issues<sup>4</sup>, then it must be reported **immediately** to the DSL, consistent with the safeguarding and child protection policy.
  - (b) If the concern or incident involves cyberbullying it should be dealt with in accordance with the School's anti-bullying policy.
  - (c) If it relates to technological controls (as described above), or to a breach of the ICT Usage policy, then it must also be reported to the ICT Coordinator.
  - (d) Other members of staff and management should be informed as appropriate in the circumstances.

<sup>4</sup> For example, it involves peer on peer abuse, sexual imagery, sexual violence and/or harassment, upskirting or radicalisation (this is not an exhaustive list, for further information see the safeguarding and child protection policy).

9.1.2 Regarding the responsibility of schools/colleges to deal with online 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:

- (a) regulate the behaviour of children when they are off the school/college site where an online safety incident is linked to the school/college
- (b) impose disciplinary penalties for inappropriate behaviour, as per the behaviour and discipline policy
- (c) search for and confiscate electronic devices, and search their contents, and where appropriate delete content (see section 7.3.9)

9.1.3 The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously. Staff should however be careful not to promise full confidentiality as information may need to be shared further (e.g. with the DSL) to determine next steps.

## 9.2 **Concerns/Incidents relating to staff**

9.2.1 **Anyone** who has **any** concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.2.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should report it **immediately** in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's child protection and safeguarding policy and procedures.

## 9.3 **Misuse by any user**

9.3.1 **Anyone** who has **any** concern about the misuse of technology by any other user should report it immediately to the ICT Coordinator and/or the DSL as relevant.

9.3.2 The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

9.3.3 If the School considers that any person is vulnerable to radicalisation, the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

## 9.4 **Cybercrime**

9.4.1 Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

9.4.2 Cyber-dependent crimes include;

- (a) unauthorised access to computers (illegal 'hacking'), for example, accessing a school's computer network to look for test paper answers or change grades awarded;
- (b) denial of service (Dos or DDoS) attacks or 'booting', which are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and
- (c) making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

9.4.3 The School is aware that pupils with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

9.4.4 If staff have any concerns about a child in this area, they should refer the matter to the DSL immediately. The DSL should then consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general online safety.

## 9.5 **Recording online safety incidents**

The School maintains a log of online safety incidents, using MyConcern as the reporting tool, which is monitored by the DSL. The reporting of online safety incidents should include the following data:

- (a) Name of person reporting the incident
- (b) Date and time of incident
- (c) Date reported
- (d) Names of people involved
- (e) Location and device details
- (f) Details of incident, including evidence where possible
- (g) Clarification of the risk or breach – e.g. does it relate to safeguarding, bullying, inappropriate content, sexting, data protection, copyright infringement...etc.? Use the 4 C's categorisation as described in 8.7.2.
- (h) Initial action taken and current status

9.6 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.

9.7 The information created in connection with this policy may contain personal data. The School's use of this personal data will be in accordance with Alpha Plus Group's data

protection and retention policies. Data in the online 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](#).

## 10 Education

- 10.1 The safe use of technology is integral to the School's curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices 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.
- 10.2 The safe use of technology is a focus in all areas of the curriculum and teacher training, and key safety messages are reinforced as part of assemblies and tutorial / pastoral activities, teaching pupils:
- 10.2.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;
  - 10.2.2 about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "*banter*" or "*just boys being boys*";
  - 10.2.3 to be critically aware of content they access online and guided to validate accuracy of information;
  - 10.2.4 how to recognise suspicious, bullying or extremist behaviour;
  - 10.2.5 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
  - 10.2.6 the consequences of negative online behaviour;
  - 10.2.7 how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and
  - 10.2.8 how to respond to harmful online challenges and hoaxes.
- 10.3 Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element.
- 10.4 Those parts of the curriculum which deal with the safe use of technology are reviewed on a regular basis to ensure their relevance.
- 10.5 The School's acceptable use policy for pupils sets out the School rules regarding the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.
- 10.6 The School delivers Online Safety to pupils. Online safety lessons are delivered half-termly to students using the Gooseberry Planet online service which covers a comprehensive curriculum of methods and advice that pupils can use to stay safe online. The PSHE curriculum follows Jigsaw which also covers methods of staying safe online. Specialist delivered interactive workshops are presented to the children annually allowing children to

experience some of these risks first hand. An assembly and a week of specialist lessons are delivered to students during the week of “Safer Internet Day”.

- 10.6.1 children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- 10.6.2 children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
- 10.6.3 children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.]

## 10.7 Useful online safety resources for pupils

- 10.7.1 <http://www.thinkuknow.co.uk/>
- 10.7.2 <http://www.childnet.com/young-people>
- 10.7.3 <https://childnet.com/resources/smartie-the-penguin>]
- 10.7.4 <https://www.childnet.com/resources/digiduck-stories>]
- 10.7.5 <https://www.saferinternet.org.uk/advice-centre/young-people>
- 10.7.6 <https://www.disrespectnobody.co.uk/>
- 10.7.7 <http://www.safetynetkids.org.uk/>
- 10.7.8 <https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/>
- 10.7.9 <https://www.bbc.com/ownit>
- 10.7.10 <https://www.gov.uk/government/publications/indecent-images-of-children-guidance-for-young-people/indecent-images-of-children-guidance-for-young-people>

## 11 Training

### 11.1 Staff

- 11.1.1 The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.
- 11.1.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy.
- 11.1.3 Ongoing staff development training includes training on technology safety together with specific safeguarding issues such as sharing nudes and semi-nudes images and or videos, cyberbullying, radicalisation and dealing with harmful online challenges and online hoaxes. Updates on online safety issues are shared as required and at

least annually via staff inset, termly Safeguarding updates, weekly staff Safeguarding updates in Pastoral meetings.

- 11.1.4 Where pupils wish to report a safeguarding concern, all staff are taught to reassure victims that they are being taken seriously and that they will be supported and kept safe. Staff are aware of the importance of their role in dealing with safeguarding and wellbeing issues, including those involving the use of technology, and understand that a victim should never be given the impression that they are creating a problem by reporting abuse, including sexual violence or sexual harassment, and nor should they ever be made to feel ashamed for making a report.
- 11.1.5 Where safeguarding incidents involve an online element, such as youth produced sexual imagery, staff will not view or forward sexual imagery reported to them and will follow the School's policy on sharing nudes and semi-nude images and videos as set out in Appendix 1 of the School's Safeguarding and Child Protection Policy and Procedures and [Searching, screening and confiscation: advice for schools](#) (DfE, January 2018). In certain cases, it may be appropriate for an authorised member of staff to confiscate the pupil's device to preserve any evidence and hand it to the police for inspection.
- 11.1.6 Staff are encouraged to adopt and maintain an attitude of 'it could happen here' in relation to sexual violence and sexual harassment and to address inappropriate behaviours (even where such behaviour appears relatively innocuous) as this can be an important means of intervention to help prevent problematic, abusive and/or violent behaviour in the future.
- 11.1.7 Staff are trained to look out for potential patterns of concerning, problematic or inappropriate behaviour and, where a pattern is identified, the School will decide on an appropriate course of action to take. Consideration will also be given as to whether there are wider cultural issues within the School that facilitated the occurrence of the inappropriate behaviour and, where appropriate, extra teaching time and/or staff training will be delivered to minimise the risk of it happening again.
- 11.1.8 Staff also receive data protection training on induction and at regular intervals afterwards.
- 11.1.9 The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.
- 11.1.10 **Useful online safety resources for staff**
- (a) <http://swgfl.org.uk/products-services/esafety>
  - (b) <https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals>
  - (c) <http://www.childnet.com/teachers-and-professionals>
  - (d) <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>
  - (e) <https://www.thinkuknow.co.uk/teachers/>
  - (f) <http://educateagainsthate.com/>



- (g) <https://www.commonsense.org/education/>
- (h) [Cyberbullying: advice for head teachers and school staff](#) (DfE, November 2014)
- (i) [Advice on the use of social media for online radicalisation](#) (DfE and Home Office, July 2015)
- (j) [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#) (DfDCMS and UKCIS, December 2020).
- (k) [Online safety in schools and colleges: questions from the governing board](#) (UKCIS, 2020)
- (l) [Education for a connected world framework](#) (UKCIS, 2020)
- (m) <https://www.lgfl.net/online-safety/resource-centre>
- (n) [Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools](#) (Childnet, March 2019)
- (o) [Myth vs Reality: PSHE toolkit](#) (Childnet, April 2019)
- (p) [SELMA Hack online hate toolkit](#) (SWGFL, May 2019)
- (q) [Teaching online safety in school: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects](#) (DfE, June 2019)
- (r) [Harmful online challenges and online hoaxes](#) (DfE, February 2021)
- (s) Professionals online safety helpline: [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk), 0344 381 4772.
- (t) NSPCC helpline for anyone worried about a child - 0808 800 5000
- (u) [Internet Watch Foundation](#) - internet hotline for the public and IT professionals to report potentially criminal online content

11.1.11 The Kent safeguarding children multi-agency partnership has produced guidance on online safety which is available here: <https://www.kscmp.org.uk/guidance/online-safety>

## 11.2

### 11.3 Parents

11.3.1 The School delivers a fortnightly newsletter of relevant Online Safety advice. The School also runs an annual talk to parents focussing on relevant issues and advice on how to deal with them in February during the week of Safer Internet Day.

11.3.2 Parents are encouraged to read the acceptable use policy for pupils with their son / daughter to ensure that it is fully understood.

#### 11.3.3 Useful online safety resources for parents

- (a) <https://www.saferinternet.org.uk/advice-centre/parents-and-carers>

- (b) <http://www.childnet.com/parents-and-carers>
- (c) <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>
- (d) <https://www.thinkuknow.co.uk/parents/>
- (e) <http://parentinfo.org/>
- (f) <http://parentzone.org.uk/>
- (g) <https://www.net-aware.org.uk>
- (h) <https://www.internetmatters.org/>
- (i) <https://www.common sense media.org/>
- (j) [Advice for parents and carers on cyberbullying \(DfE, November 2014\).](#)
- (k) <http://www.askaboutgames.com>
- (l) <https://www.ceop.police.uk/safety-centre>
- (m) [UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use \(February 2019\)](#)
- (n) [LGfL: parents - scare or prepare](#)
- (o) [Thinkuknow: what to do if there's a viral scare online](#)

## 12 Risk assessment

- 12.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.
- 12.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.
- 12.3 The Head has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.
- 12.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Head of IT.