E-safety Policy

Primary person responsible for this policy: James Kidd **Job title:** Vice Principal (Pastoral) **Email:** James.kidd@dld.org **Last review date:** July 2021 **Next review date:** July 2022

Circulation: This policy has been adopted by the governors and is available to parents on request. It is addressed to all members of staff and volunteers and applies wherever they are working with children.

'Parents' refers to parents, guardians and carers.

Contents

Scope and definition

This policy is part of our strategy for safeguarding children within our care. It complies with *Keeping Children Safe in Education*[1].

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.

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[2]
ICT Coordinator	Meryam Moujdi
On-site Engineer[3]	Bruce McCubbin, Auzan Malik (Apprentice)
Curriculum - ICT	Not applicable
Curriculum - PSHEE	Myles Blair
Staff Training & CPD	Thomas Hadcroft
Development of Parental Awareness	James Kidd

<u>Clarification of the relationship between the ICT Coordinator and the On-Site Engineer</u>

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/college staff is nominated as ICT Coordinator and is assigned responsibility for monitoring the effective delivery of these services on behalf of all school/college users, and for reporting problems where necessary.** The ICT Co-ordinator may well be also responsible for the ICT curriculum, but it is important that these two responsibilities are clearly understood as separate functions.

[1] It will comply with Keeping Children Safe in Education 2020

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

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

Roles in E-Safety

Principal

- Has overall responsibility for online safety provision.
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with APG and national recommendations and requirements.
- Ensures the school follows APG polivies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection.
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities.
- Ensures that all staff receive regular, up to date and appropriate online safety training.
- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, APG and national support.
- Receives regular reports from the DSL on online safety.
- Ensures that online safety practice is audited and evaluated regularly in order to identify strrengths and areas for improvement.

DSL

- Takes day to day responsibility for online safety.
- Promotes an awareness of and commitment to online safety throughout the school community.
- Acts as the named point of contact on all online safety issues, and liases with other members of staff or other agencies, as appropriate.
- Liases with the DDSL's to ensure the online safety component of the curriculum is kept under review, in order to ensure that it remains up to date and relevant.
- Liases with the DH (Staff & Operations) to facilitate training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Reviews the internet monitoring report regularly.
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends.
- Reports regularly to the Head and SLT on the incident log, internet monitoring report, current issues and developments in legislation.

Staff managing the technical environment

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Keep up to date with the school's online safety policy and technical information in order to carry out their online safety role effectively and to inform and update others as relevant.

- Provide technical support to the DSL and leadership team in the implementation of online safety procedures.
- Ensure that the school's filtering policy is applied and updated on a regular basis, and the monitoring report is run and passed to the DSL on a monthly basis (as a minimum).
- Report any filtering breaches or other online safety issues to the DSL, Principal, APG and other bodies, as appropriate.
- Ensure that any safeguarding concerns are reported to the DSL, in accordfance with the school's safeguarding procedures.

All school staff

- Read, adhere to and help promote the online safety policy, Acceptable Use Agreementa and other relevant school policies and guidance.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model safe, responsible and professional behaviours in their own use of technology.
- Embed online safety in their teaching and other school activities.
- Supervise, guide and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant).
- Have an up to date awareness of a range of online safety issues and how they may be experienced by the children of their care.
- Identify online safety concerns and take appropriate action by reporting to the DSL.
- Know when and how to escalate online safety issues.

Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities)

- Engage in age appropriate online safety education opportunities.
- Respect the feelings and rights of others both on and offline, in and out of school.
- Take responsibility for keeping themselves and others safe online.
- Report to a trusted adult, if there is a concern online.

Parents

- Support the school in online safety approached by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home.
- Model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they of their child encounter risk or concerns online.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

External groups

- Any external individual/organisation must sign an Acceptable Use Agreement prior to being given individual access to the school network.

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 radicalization,
2. The corruption of young minds through the normalization of disrespectful, or anti-social language and behaviour through exposure to age-inappropriate content[4], 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,
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'):

[4] 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.**

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 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 (Computing) and PSHEE 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.

<u>Education and Engagement</u>

- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to compliment online safety education in the curriculum
- Educating pupils in the effective use of the internet; including the skills of knowledge location, retrieval and evaluation (online safety, digital footprint) – IT Induction/Training
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- How to respect copyright when using material from the internet
- Supporting pupils in building resilience to radicatlisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in devision making

PSHE

We utilise a programme called Jigsaw for or statutory PSHE which includes content around E-Safety.

Additional PSHE content is provided in Tutor Periods in sessions for events such as Safer Internet Day.

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/college. Foremost amongst these are:

a) Children to whom we provide bespoke[5] 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 Coordinator. Any member of the school/college 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/college operates.

The filtering system produces a report which identifies attempts to access sites that may give rise to concern. This report should be run on a monthly basis (as a minimum). Monitoring can also be undertaken on a needs basis. Concerns identified through monitoring will be managed by the DSL depending on the nature of the issue.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils: effective classroom management and regular education about safe and responsible use is essential. All users are informed that use of school systems is monitored and that all monitoring is in line with GDPR, human rights and privacy legislation.

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

Whilst these filtering controls can similarly apply to mobile phones which use the school/college 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 separate policy document).

Our staff are authorised to search for[6] 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/College 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.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils: effective classroom management and regular education about safe and responsible use is essential. All users are informed that use of school systems is monitored and that all monitoring is in line with GDPR, human rights and privacy legislation.

Managing the IT Infrastructure

- Has secure broadband connectivity
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Ensures network is healthy through use of anti-virus software and network set-up so staff and pupils cannot download executable files
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network
- Ensures all staff and students have signed an acceptable use agreement
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of VLE as a key way to direct pupils to age / subject appropriate web sites
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the Deputy Head Pastoral and Wellbeing
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the Police

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

Network Management (user access, backup)

- Uses individual, audited log-ins for all users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed;
- Stores all data within the school in a manner that conforms to the UK data protection requirements
- Ensures staff read and sign that they have understood the school's e-safety Policy Following this, they are set-up with Internet, email access and network access. Online access to the School network is through a unique, audited username and password
- We provide pupils with an individual network log-in username. They are also expected to use and protect a personal password
- All pupils have their own unique username and password which gives them access to the Internet, and their own school approved email account
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day to save energy
- Has set-up the network so that users cannot download executable files / programmes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities
- Maintains equipment to ensure Health and Safety is followed; equipment installed and checked by approved Suppliers
- Has integrated curriculum and administration networks, but access to the Management Information System (SIMS) is set-up so as to ensure staff users can only access modules related to their role
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems
- Does not allow any outside Agency to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or SIMS Support, parents using a secure portal to access information on their child
- Provides pupils and staff with access to content and resources through The VLE which staff and pupils access using their username and password
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data
- Uses our broadband network for our CCTV system

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains high
- Reviews the school IT systems regularly with regard to health and safety and security

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff to use a mixture of uppercase, lowercase and numerical characters e.g. tSMQ79bY would suffice

Email

- Provides staff with an email account (an Office 365 account) for their professional use, and makes clear personal email should be through a separate account
- Does not publish personal e-mail addresses of pupils on the school website
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of ISP recommended technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

School website

The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained, as well as the Marketing & Communications Manager. Uploading of information is restricted to our website authorisers. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status. Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Learning platform (VLE)

Uploading of information on the schools' Virtual Learning Platform (Canvas). The VLE is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas. Photographs and videos uploaded to the VLE will only be accessible by members of the school community.

Social networking
Teachers are requested not to run social network spaces for student use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications. It is strongly recommended that in private use no reference should be made in social media to pupils, parents or school staff. They must not engage in online discussion on personal matters relating to members of the school community. Personal opinions should not be attributed to the School. Security settings on personal social media profiles must be regularly checked to minimise risk of loss of personal information.

CCTV
We have CCTV in the school as part of our site surveillance for staff and pupil safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

Parental responsibilities and off-site E-safety

Given that children's engagement with the digital world extends well beyond the school/college 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 encourage parents to attend these where possible.

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/college 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[7], 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.

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

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.

This policy links to:

- IT Usage Policy
- Social Media, Mobile Phone and Student Photograph Policy.
- PSHEE Policy
- Safeguarding Policy
- Anti-Bullying Policy
- Prevent Policy
- Staff Conduct Policy
- Remote Teaching and Learning Policy