ABBEY COLLEGE MANCHESTER

Alpha Plus group
the Gold Standard in education

E-safety Policy

Primary person responsible for updates to this policy: Liz Elam

Job title: Principal

Last review date: May 2021

Next review date: June 2022

Relevant ISI coding (if applicable)

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

Appendices

Scope and definition

This policy is part of our strategy for safeguarding children within our care. It complies with *Keeping Children Safe in Education 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
- ICT Usage
- PSHEE
- Mobile Phones, Photos and Images
- 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]
ICT Coordinator	Carole Keogh
On-site Engineer[2]	Carole Keogh
E-Safety Officer	Nigel Willetts
Curriculum - ICT	Martin Smitheman
Curriculum - PSHEE	Chris Randell
Staff Training & CPD	Liz Elam
Development of Parental Awareness	Chris Randell

Clarification of the relationship between the ICT Coordinator 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/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.

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

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

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[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,
7. The lasting damage to self-esteem and to reputation which children may incur (to themselves or to others, thoughtlessly or maliciously) by distributing or publishing confidential, insensitive, offensive or otherwise inappropriate content,
8. Exposure to fraud, hacking or identity-theft through insufficient security of passwords and personal details,
9. The use of new media and technology in distracting or addictive ways.

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

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

Key principles and controls

We take E-safety very seriously. In addition to all the general safeguarding principles and controls included within our *Safeguarding policy*, the over-arching principle with E-safety is the need to educate 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

[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.**

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 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.

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[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 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.

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, 4G and 5G signals. Please see the Mobile Phones and Devices Policy for guidance on mobile phone usage.

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

[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*** (2018).

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 (e.g. sexting) should not be deleted prior to giving the device to the police. **If staff suspect that a device may contain illegal images (e.g. sexting), they must not look at these images but pass the device to the DSL who will liaise with the police as appropriate.**

The 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.

Parental responsibilities and off-site E-safety

Given that children's engagement with the digital world extends well beyond the 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[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 Coordinator.

Other members of staff and management should be informed as appropriate in the circumstances.

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

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

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

Once investigated, a record of the resolution of the incident, and actions taken as a result, must be maintained. Such records should be readily available for inspection during governance visits.

Data in the E-safety log will be processed in line with Alpha Plus Group's Privacy Notice, which is available on request or can be accessed via the Group's public portal.

Appendix 1 – e-Safety Procedure for Incidents Involving Students

- All eSafety incidents must be recorded using form ESI1; this can be handwritten or sent as an e-mail attachment to the DSL (Designated Safeguarding Lead), Chris Randell.
- Acknowledgement of receipt will be given to the reporting member of staff.
- All reported incidents will be followed up and assessed by the SLT, the HOH, a Safeguarding Lead (DSL/DDSL) and the ICT and Database Manager/E-Safety Officer.
- A group of relevant members of staff and/or outside agents may meet to decide on the best possible course of action
- High-priority incidents will be acted upon as soon as possible by a member of the SLT and or the DSL; outside agencies and parents/guardians will be informed immediately by a member of the SLT where required
- Any actions taken and outcomes following reporting will be recorded and stored with the original eSafety report and on the student file
- If it is a child protection issue, notes will be stored in the DSL's office and a file note placed on the student file
- Immediate suspension or restriction of student ICT privileges will be put into place where it is warranted.
- The students involved may also be subject to disciplinary procedures—possibly effective immediately—as laid down in the student disciplinary code.

Appendix 2 – Student e-Safety Incident Initial Report Form

Form ESI1

Student eSafety Incident Initial Report Form

This form must be completed as far as is practicable and handed to the DSL for storage and referral as soon as possible after the disclosure. Incidents or allegations involving staff should be reported immediately to the relevant line manager and/or the principal.

Date of the incident: (dd/mm/yyyy)	
Time:(hh:mm)	
Name of staff member(s) recording the incident:	
Staff/students affected by the incident and/or witnessing it.	
Names of those suspected of involvement or known to be involved.	
Initial assessment of the incident (more than one may apply:	Cyberbullying □ Child Protection Issue □ Hacking □ Malware (viruses etc.) □ Indecent Images □ Racist Material □ Misuse of Personal Information □ Financial/Fraud □ Other □
Incident location (e.g. building/room)	
Machines/equipment involved in the incident (e.g. student laptop)	
Brief description of the incident: *(For confidential information to be seen only by any of the SLT, Child Protection Team, ICT and database manager and eSafety advisor, please complete a separate sheet marked as confidential, attach it to a copy of this form and hand it to a designated person)*	
Evidence gathered (e.g. printouts, screenshots, USB Flash Drive, Laptop) *Evidence must be passed to SLT or other designated person for secure storage.*	

Action taken immediately: (e.g. switched off the laptop or removed the USB flash drive.)	
Details of any advice given immediately after the reporting of the incident (e.g. change ‘phone number, contact social networking site admin)	
Date : (dd/mm/yyyy)	
Signature of primary reporter:	

Office Use Only

Date:

High priority	Yes / No

Supplementary Material	Yes / No

Action(s):

SLT involved	
Contacted police	
Contacted parent/guardian	
ICT and database manager informed	
DSL involved	
eSafety advisor informed	
Head of House informed	