KAPLAN INTERNATIONAL

E- Safety Policy

Document Control			
Document type	Policy		
Document owner	Stephen Spick – Head of Information Security & Compliance		
Business area	Information Security and Compliance		
Document status	Published		
Version	V4.1		
Approved by	Stephen Spick	Date	31st March 2025
Job Title	Head of Information Security and Compliance	Signature	Signed by: stephen Spick 750BBCBB6ED3499...
Approved by	Rachel Convery	Date	31st March 2025
Job Title	General Counsel	Signature	DocuSigned by: Rachael Convery 037F29D7DBBD4B5...
Distribution	All users of Kaplan Information Systems.		
Date of publication	March 2025	Next review date	
Date of original publication	July 2021	Revision frequency	Annual
Superseded documents	E-safety policy v4.0		
Related documents			

Table of Contents:

1 Introduction

It is the duty of the school / college to ensure that every student in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world.
Increasingly, minors and vulnerable adults are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

Information and Communications Technology (ICT) in the 21st Century has an all-encompassing role within the lives of minors and adults. Current and emerging technologies used in school / college and, more importantly in many cases, used outside of school / colleges by minors, vulnerable adults and students include**:**

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smartphones and Tablets.

The widespread use of digital communications technologies, as listed above,presents young people with a lot of opportunities for learning, participation, creativity and self-expression. At the same time, it poses a range of safeguarding concerns, which can be grouped as follows:

Content
Student exposure to illegal, inappropriate or harmful online content including spam, pornography, substance abuse, violence, cyber-bullying, extremism and hate sites, and lifestyle sites that promote eating disorders, self-harm or suicide.

Contact
Students participate in Exploitative digital communication including viruses and malware, personal data or identity theft, cyber-stalking, online grooming, anonymous online chat sites and cyber-bullying.

Conduct
Concerns for students' health and well-being, such as gaming, gambling or social network addiction; online disclosure of personal information and ignorance of privacy settings; online reputation and 'sexting' (sending and receiving personally intimate digital images); and illegal conduct, including hacking, plagiarism, and

copyright infringement of digital media, such as music and film.

E-safety is a shared responsibility; all staff, students, residence staff and, where applicable host families, are encouraged to work together to develop strategies to promote a safeenvironment. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' understanding the risks to which that they may see, so that they have the confidence and skills to face and deal with these risks.

2 Purpose

The requirement to ensure that minors and vulnerable adults can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in school / colleges are bound. The purpose of the e-safety policy is to help to ensure safe and appropriate use. Kaplan International aims to adopt the highest possible standardsand to take all reasonable steps in relation to the safety and welfare of all students.

This Policy is based on, and incorporates, but is not limited to, elements of the legislation and national guidance documents listed in Appendix-A below.

3 Scope

This E-safety policy together with the Social Media Policy applies to everyone working at or attending Kaplan. It imposes responsibilities on all staff, students, agency staff and volunteers, contractors, visitors, consultants and those working under self-employed arrangements. It shares the use of technology both on and off the school / college premises and where there is a risk to the safety of students.

4 Policy Statement

The aim of the E-Safety policy is to create and maintain a safe, healthy and supportive learning and working environment for our students, staff and visitors. The aims of this policy are:

- to encourage students to make good use of the education opportunities presented by access to the internet and other electronic communication.
- to safeguard and promote the welfare of students by preventing cyber-bullying and other forms of abuse.
- to ensure students use technology safely and securely.
- to help students take responsibility for their own e-safety; and
- to minimise the risk of harm to the assets and reputation of the school / college.

Kaplan and its school / colleges will take all reasonable measures to ensure that users accessonly appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable materialwill never occur via a school / college computer. The school / college does not accept liability for the material accessed, or any consequences resulting from Internet use.

The use of computer systems without permission or for inappropriate purposes may result in a criminal offence being committed under the Computer Misuse Act 1990. Any suspected breaches of the Computer Misuse Act 1990 will be reported to the Police.

Methods to identify, assess and minimise risks will be reviewed regularly.

Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Personal Data will be recorded, processed, transferred andmade available according to the UK General Data Protection Regulation and Data Protection Act 2018.

If a partner university provides Wi-Fi, students must be registered with the University's network. All students receive guidance on the use of the internet and email systems available in the School / College. If at any time they are unsure about correct usage, they must seek assistance from a member of staff.

5 Responsibilities

Senior Management Team

The Senior Management Teams are responsible for:

- Making sure this Policy is implemented across Kaplan.
- that the school / college follows all current e-safety advice to keep students and staffsafe.
- the overall e-safety provision across Kaplan.
- data and data security.
- liaising with the Local Authority and other relevant agencies where required, and delegating the day-to-day management of e-safety to the Principals /College Directors and Designated Safeguarding Leads of schools / Colleges.

Principal / College Director and Designated Safeguarding Lead

Principals / College Directors and Designated Safeguarding Leads are responsible for:

- for e-safety issues and have a leading roles inestablishing and reviewing the school / college e-safety

policies / documents;

- promoting awareness and commitment to e-safeguarding throughout the school / college community.
- liaising with ICT technical staff; and
- remaining regularly updated on e-safety issues and legislation and awareness of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal or inappropriate materials, inappropriate on-line contact with adults or strangers; potential or actual incidents of grooming; cyber bullying and use of social media.

Teaching & Support Staff

Teaching and Support Staff are responsible for:

- maintaining up-to-date awareness of e-safety matters and of the current school / college e-safetypolicy and practices.
- ensuring they and the students they support adhere to the IT Acceptable Use Policy.
- making students aware of and adhere to the school / college e-safety and acceptable usage policies.
- monitoring ICT activity in lessons, extracurricular and extended school / college activities: and
- Ensuring that in lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students

Students are responsible for:

- using the school / college ICT systems in accordance with the Acceptable Usage Agreement, which they will be required to sign before being given access to school / college systems. Parents will be required to read through and sign alongside their child's signature:
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- reading and agreeing to the school / college policy on the taking, the use of images and on cyber-bullying; understanding the importance of good e-safety practice when using digital technologies out of school / college; and
- for learning about the benefits and risks of using the Internet andother technologies both in school / college and at home.

6 Reporting incidents & Procedure

E-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers play a very important role, their observation of behaviour is essential in recognising concerns about Students and in developing trust so that issues are reported.

Students should report to the Designated Safeguarding Lead (DSL) if: they are troubled by something they have been exposed to on the internet; or they have evidence of an incident of wrong-doing by another user, either on the school / college network or outside it, where the behaviour could threaten someone's safety or welfare.

Similarly, staff and host families should report their concerns to the DSL, who will follow procedure with the relevant school / college policies for Safeguarding. Staff should also consider the Whistleblowing policy for procedure on how to report within theorganisation.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the school / college will determine the level of response necessary for the offence disclosed. Following disclosure of this information this will need to be immediately reported to the Senior Management Team by the school / college and or the DSL. The decision to involve Police will be made by the Senior Management Team and will be made as soon as possible, after contacting the Local Authority Designated Officer (LADO), if the offence is deemed serious enough that the school / college need to report it to the police.

All members of the school / college community will be informed about the procedure for reporting e-Safety concerns.

The DSL will be informed of any e-safety incidents involving Child Protection concerns, which will then be escalated appropriately.

Where appropriate the school / college will manage e-safety incidents in accordance with the school / college behaviour policy.

The school / college will inform parents/ guardians/ carers/ host families of any concern asand when required.

After any investigation is completed, the school / college will go through the facts, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school / college will contact the Senior Management team who will then inform the Police of the concern if required.

7 Staff Induction

All new staff will be provided with information and guidance on e-safety and the school / college's Acceptable Usage Policies.

The following websites are recommended as further general guidance concerninge-safety: http://www.thinkuknow.co.uk/ and https://www.getsafeonline.org/

8 Management of Social Media & Social Networking

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Theyshould be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. *S*taff who publish inappropriate material either in the course of their employment or in a personal capacity may face disciplinary procedures.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school / college) will be raised with their parents/ guardians/ host families, particularly when concerning students' underage use of sites at their residential accommodation.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour as outlined in the Kaplan International IT Acceptable Usage Policy.

9 Cyber Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" - DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When minors and vulnerable adults are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects.

A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school / college and residence staff, parents and carers/ host families understand how cyber bullying is different from other forms of bullying, how it can affect people and

how to respond and try to stop this from happening. Promoting a culture of confident users will support innovation and safety. Where bullying outside school / college (such as online or via text) is reported to the school / college, it must be investigated and acted on. Although bullying is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If staff feel that an offence may have been committed, they should inform the Senior Management Team who will contact the police where appropriate.

Cyber bullying (along with all other forms of bullying) of any member of the school / college community will not be tolerated.

All incidents of cyber bullying reported to the school / college will be dealt with appropriately.

Students, staff, residence accommodation staff and host families will be advised to keep a record of any bullying they become aware of.

The school / college will take steps to identify accused bully, where possible and appropriate. This may include examining school / college system logs, CCTV, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Students, staff, residential accommodation staff and host families will be requiredto work with the school / college to support the approach to cyber bullying and the school / college's e-Safety policy.

Sanctions for those involved in cyber bullying may include:

- the bully will be asked to remove any material that is to be inappropriate or offensive.
- an internet service provider or host may be contacted to remove content if the bullyrefuses or is unable to delete content.
- other school / college sanctions for students and staff may also be used in accordance with the Safeguarding Policy and Terms and Conditions.
- Parents/guardian/ host families of Students being informed; and/or
- the police will be contacted by the Senior Management team if a criminal offence issuspected.

10 Revenge Pornography

Sharing private material as "revenge porn" online is illegal in England and Wales under the CriminalJustice and Courts Bill 2015. The legislation defines revenge pornography as the publication of explicit material portraying someone who has not allowed the image or video to be shared. The law makes it illegal to disclose a "*private*

sexual photograph or film" without the consent of the person in the content, and with the *intent to cause them distress*. It is not an offence for the person to show the photograph or film to the individual.

Where illegal activity has taken place or is taking place involving students the school / college will determine the level of response necessary for the offence disclosed. Following disclosure of this information this will need to be immediately reportedto the Senior Management Team by the Principal / College Director and DSL. The decision to notify the police will be made by the Senior Management Team.

11 Radicalisation & Extremism

Kaplan is committed to having "*due regard to the need to prevent people from being drawn into terrorism*" in accordance with the Counter Terrorism and Security Act 2015 known as the Prevent duty. Whilst this is a standalone policy, it is integral to our Prevent Policy and should be applied as an extension to the school / colleges' current and established policies and procedures that cover this area.

If staff become aware of or see signs of conflict, aggressive or extreme behaviour or opinions held by a student or group of students they must inform the school / college Prevent Lead and the Principal / College Director. The Principal / College Director will immediately inform the KI Prevent lead and Senior Management Team who will decide a course of action.

Students may become susceptible to radicalisation through a range of social, personal and environmental factors. All students are provided with information and reminded of the prevent duty as part of their induction.

Students are reminded that they cannot access or otherwise interact with the internet or social media which promotes, encourages or supports extremism, radicalisation and or facilitates terrorism on Kaplan Technology Systems or personal devices. Doing so will result in students being banned from the use of Kaplan computers and Kaplan Technology System networks and reported to the police.

Kaplan expect students not to use their personal devices outside school / college hours to access material that promotes, encourages or supports extremism, radicalisation and or facilitates terrorism. If Kaplan become aware of such activity it will be reported to the police.

Kaplan is committed to having "due regard to the need to prevent people from being drawn into terrorism" in accordance with the Counter Terrorism and Security Act 2015 known as the Prevent duty. Whilst this is a standalone policy, it is integral to our Prevent Policy and should be applied as an extension to the school / colleges' current and established policies and procedures that cover this area.

If staff become aware of or see signs of conflict, aggressive or extreme behaviour or opinions held by a student or group of students they must inform the school / college Prevent Lead and the Principal. The Principal will

immediately inform the KI Prevent lead and Senior Management Team who will decide a course of action.

12 Monitoring & Review

The Head of Information Security & Compliance and Senior Management Team are responsible for reviewing this Policy, considering any incidents that have occurred, new technologies, in accordance with government guidance, and in consultation with students, parents and staff.

13 Review and Maintenance

This policy will be reviewed annually unless there is significant change.

14 History Log

Version	Date	Description of Changes	Author and/or Reviewer
1.0	July 2021	Draft Policy	Sue Edwards & Electra Lamaj
2.0	June 2022	Annual Review	Howlader Kamrul Hassan & Electra Lamaj
3.0	April 2023	Annual Review	Electra Lamaj
4.0	October 2023	Combination of policy for both Kaplan Languages and Kaplan Pathways	Alex Fowler, Sue Edwards, Stephen Spick
4.1	March 2025	Annual document review	Karen Handyside

APPENDIX- A: legislation and national guidance documents

- Racial and Religious Hatred Act 2016
- Counter-Terrorism & Security Bill 2015
- Criminal Justice Act 2003
- Sexual Offences Act 2003
- Communications Act 2003
- UK General Data Protection Regulation
- Data Protection Act 2018
- The Computer Misuse Act 1990
- Malicious Communications Act 1998
- Public Order Act 1986
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Criminal Justice and Immigration Act 2008
- Education and Inspections Act 2006

The E-safety Policy should be read in conjunction with the following policies:

- Safeguarding Policy
- Whistleblowing Policy
- Prevent Policy
- IT Acceptable Use Policy