Kaplan UK – Information Security Documentation

Acceptable Use Policy

1 Document History

1.1 Document Location

This document is located in: \PPP\ISSG ISMS Documents

1.2 Revision History

Revision Date	Version	Primary Author(s)	Summary of changes
25 Aug 2010	1.0	Michael Collins	Adapted from US AUP
11 Aug 2011	1.2	Michael Collins	Update to IT Security Personnel and contacts
21 Sep 2012	1.3	Michael Collins	Included Data Classification references
02 Oct 2013	1.4	Michael Collins	Reformatted in line with latest US AUP
17 Feb 2016	1.5	Anton Scipio	Update to Approvals and Distribution list, grammar check and addition of comments
17 Nov 2017	1.6	Simon Caldow	Update for GDPR Provision, replacement of named roles with titles. Consistent formatting.
30 Oct 2018	1.7	Ashish Gangar	Reviewed and updated for ISO 27001 and DPA 2018 compliance
10 Dec 2019	1.8	Ashish Gangar	Annual review and added reference to Information Security Policy

1.3 Approvals

This document requires the following approvals.

Role	Signature	Date of Issue	Version
Chief Technology Officer	AG	10 Dec 2019	1.8
Head of IT Service Operations	CH	10 Dec 2019	1.8
IT Security & Compliance Manager	Ashish G	10 Dec 2019	1.8

1.4 Distribution

Title	Purpose	Date of Issue	Version
Chief Technology Officer	Review	10 Dec 2019	1.8
Head of IT Service Operations	Review	10 Dec 2019	1.8
IT Security & Compliance Manager	Review	10 Dec 2019	1.8
Head of Applications	Info	10 Dec 2019	1.8
Application & Data Architect	Info	10 Dec 2019	1.8
Head of Engineering	Info	10 Dec 2019	1.8
Head of Analysis & Testing	Info	10 Dec 2019	1.8
Head of Projects	Info	10 Dec 2019	1.8
Legal Counsel (Kaplan UK)	Info	10 Dec 2019	1.8
Head of Human Resources (Kaplan UK)	Info	10 Dec 2019	1.8

2 Table of Contents

3 Purpose

The purpose of Kaplan's Information Technology Acceptable Use Policy ("AUP") is to prescribe the set of guidelines by which Kaplan IT Assets may be used by the employees, independent contractors, vendors and other users ("Users") with access to Kaplan's information technology hardware, software, networks, telephone systems, mobile communications devices, and all other aspects of the information technology systems ("Kaplan Technology Assets") of Kaplan, Inc. and each of its business units, including Kaplan UK & Ireland (collectively, "Kaplan"). The goal of this Policy is to protect the Kaplan Technology Assets and the information contained in the Kaplan Technology Assets from misuse.

Understanding and complying with this AUP is mandatory for all Kaplan Users.

4 Policy

4.1 User Responsibility and Compliance

4.1.1 Rules and obligation

The rules and obligations described in this policy apply to all Users of the Kaplan Technology assets and is within the organisation ISMS Policy. It is each User's duty to use the Kaplan Technology assets responsibly, professionally, ethically, lawfully, and conduct their activities accordingly.

4.1.2 Application

This policy shall be applied by the personnel at each business unit who are responsible for managing and protecting the Kaplan Technology assets and who are listed on Appendix A to this Policy ("Divisional IT Staff"), with oversight from the Information Security Steering Group at Kaplan.

4.1.3 Violations

Violations to this policy by staff, student or contractors can result in immediate withdrawal or suspension of system and network privileges for individuals. Restoration of security privileges may be dependent on re-awareness training and upon approval from the security and compliance team. Where a criminal offense has been committed, Kaplan reserves the right to advise law enforcement agency.

4.1.4 Variation

Kaplan reserves the right to modify, amend, or terminate any stipulation of this AUP at any time.

This Policy does not create a contract of employment and does not alter the status of any employee, independent contractor, vendor or other user.

4.2 Use of Kaplan Technology assets

4.2.1 Don't Transmit or Store Improper or Unlawful Material

Users are strictly prohibited from storing, transmitting, or printing any improper materials on the Kaplan Technology Assets. "Improper Materials" may include, but are not limited to, materials that (a) infringe the proprietary rights of another person, (b) contain commercial or personal advertisements, solicitations, promotions, or political material; (c) contain viruses or other destructive programs; (d) are harassing, embarrassing, sexually explicit, profane, obscene, intimidating, or defamatory, or (d) constitute fraud, or are otherwise unlawful. Users may not transmit Improper Materials by e-mail or any other form of electronic communication, such as fax, newsgroups, chat groups, instant messenger. Users may not display or store Improper Materials in any part of the Kaplan Technology assets.

4.2.2 Don't Misuse the Kaplan Technology assets

Users may not use the Kaplan Technology assets for non-business related activities, such as (but not limited to) (a) sending non-business related mass distribution emails or chain letters, (b) subscribing to non-business related mailing lists, (c) spending excessive amounts of time browsing the Internet, visiting social networking sites or chatting via instant messaging programs, (d) visiting Internet chat rooms, (e) gambling on the Internet , (f) participating in online sports, (g) using Internet auction sites, (h) downloading any material from peer-to-peer file-sharing networks such as Morpheus or Kazaa, (i) playing computer games, (j) accessing or using Kaplan technology for terrorism related activities or (k) engaging in hacking activity.

4.2.3. Identify Yourself Accurately in Communications

Users must identify themselves honestly and accurately when sending email. Users may not alter the "From" field or any other attribution-of-origin field in email messages, or postings. Users may not communicate through the Kaplan Technology assets either anonymously or under a pseudonym.

4.2.4 Limit Personal Use

Kaplan is aware that Users may send personal communications through the Kaplan technology assets. Kaplan expects users to limit such personal use to a minimum.
You are strictly prohibited from making any personal use of the Kaplan Technology that (a) absorbs large amount of the System resources, (b) distracts you from your duties, or (c) Kaplan, in its sole discretion, considers excessive.

4.2.5 Use the Internet Cautiously

Users should exercise caution when browsing the Internet through the Kaplan Technology assets. In order to avoid receiving unsolicited email or email containing offensive content, Users should avoid posting their Kaplan Technology assets email addresses on the Internet. Kaplan implement Internet blocking software to prevent receipt of unsolicited email or to restrict access to inappropriate Internet sites based on category (including but not limited to abused-drugs, adult, command-and-control, extremism, gambling, hacking, malware, phishing, questionable, weapons), however, Kaplan is not responsible for such material.

4.2.6 Obey Copyright Laws

Users may not use the Kaplan Technology assets in a manner that infringes the copyright rights of others. Copyright law protects the exclusive rights in images, music, text, audiovisual materials, software, and photographs. The distribution, display, performance, or reproduction of any copyright protected material through the Kaplan Technology assets without the permission of the copyright owner is strictly prohibited.

4.2.7 Comply with Software Licenses

The Kaplan Technology assets include software that is licensed from third parties. Users must use any licensed software in accordance with the terms of the licensing agreement. Users may not reproduce or install any software that has not been properly authorised or purchased by the Divisional IT Staff, Kaplan IT Management, or other authorised personnel. No User may modify, revise, recompile, disassemble, reverse engineer, or otherwise alter any software licensed to Kaplan without prior written authorisation from the software vendor and Kaplan.

4.2.8 Conserve Resources

Storage space on the Kaplan Technology assets is not an unlimited resource, and Users should take all possible steps to conserve the storage space.

4.2.9 Systems capability

Users should delete unnecessary or unwanted files on a regular basis from network servers, email inboxes and folders, and local hard drives.

4.2.10 No unauthorised software

Users may not reproduce or install on the Kaplan Technology Assets any software that has not been properly authorised, licensed or purchased by Kaplan.

4.2.11 Do not Access without Permission

Only Users who have been given approval or authorisation to use Kaplan Technology Assets are permitted to do so. Users should only access those Kaplan Technology Assets for which they have permission, even in cases where Users might have the ability to access certain Assets for which they do not have permission.

4.2.12 Do not take unauthorised photos/screenshots

Users may not capture screenshots or take photographs of screens or documents that contain sensitive information. In the case of the Kaplan infrastructure unless approved by senior management users are not permitted to take pictures of the Kaplan infrastructure.

5 Privacy

5.1 Fundamentals

5.1.1 No Expectation of Privacy

Users should have no expectation of privacy in anything created, stored, sent, or received on the Kaplan Technology assets. User accounts on the Kaplan Technology assets are issued to individuals to assist them in the performance of their jobs, and remain the property of Kaplan. Users are permitted to access the Kaplan Technology assets for the purpose of conducting Kaplan business, and personal use should be limited and is not private.

5.1.2 Use May Be Monitored

Divisional IT Staff, Kaplan IT Management and limited others such as members of the Human Resources and Legal departments have access to and may review any information that Users create, store, send, or receive on the Kaplan Technology assets, including email and instant messages, and communicate such information to others. Deleting emails and IM messages does not remove this information from the servers within the Kaplan Technology assets.

5.1.3 Blocking Software

Kaplan may implement Internet blocking software to restrict access to inappropriate Internet sites or prevent the receipt of suspicious emails.

5.2 Protection of Kaplan's Confidential Information

5.2.1 What is Confidential Information?

Users who have access to Kaplan's confidential information must be careful to protect such information from disclosure to unauthorised recipients. "Confidential Information" includes, but is not limited to, financial information, business plans, marketing plans, software source and object code, and contracts.

5.2.2 How to Protect Confidential Information

In order to prevent unauthorised individuals from viewing such information, Users should exercise proper judgment when sending Confidential Information via email or forwarding email strings containing Confidential Information.

5.2.3 What is Personally Identifiable Information?

Certain types of Confidential Information are highly sensitive and must be protected with the utmost security (Personally Identifiable Information (PII)), because unauthorised disclosure creates the most harm to the owner and greatest legal liability to Kaplan. Personally Identifiable Information includes, but is not limited to the following the following:

- Names
- Addresses
- Date of Birth
- National insurance numbers
- Credit card numbers
- Driver's license numbers
- Bank account numbers
- Passwords and logins
- Personal health information, relating to physical and/or mental health
- Information about sexual activity or orientation
- Information about race or ethnicity
- Information about political opinions
- Information about religious or philosophical beliefs
- Information about trade-union membership
- Student (customer) or lead email addresses
- Student (customer) phone numbers
- Students' Kaplan ID number
- Students' registration number with an awarding body
- Information about the commission or alleged commission of an offence;
- Information about any proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5.2.4 How to Protect Personally Identifiable Information

Access to Personally Identifiable Information should be strictly dependent on authorisation by the Information/ Asset owner. Do not attempt to gain access to Personally Identifiable Information unless you are authorised to do so.

5.2.5 Report Breaches

You should immediately report any unauthorised or accidental disclosure of Confidential or Personally Identifiable Information through the Incident Reporting Procedure in Section 6

5.2.6 Data Protection Act & General Data Protection Regulations

Kaplan UK & Ireland is subject to the Data Protection Act 2018 ("DPA") and from 25 May 2018 the General Data Protection Regulation ("GDPR") which establishes frameworks of rights and duties designed to protect personal data.

5.3 Logins and Passwords

5.3.1 Login Accounts

Users may be assigned a unique login account consisting of a UserID and password, their Kaplan Login. Users are responsible for all transactions made using his or her Kaplan Login. No one may access the Kaplan Technology assets by entering another User's Kaplan Login. All Users are expected either to lock up or log off the workstation when they are away from their work area for extended periods of time, and to log off their workstation before leaving for home at the end of each business day, unless the logoff interferes with an application or normal operation running on the workstation. Users may not disguise their identity while using the Kaplan Technology assets.

5.3.2 Password Security

Users are responsible for safeguarding their Kaplan Login password. Individual passwords should not be printed, stored online, posted on sticky notes, or shared with others. Users are prohibited from using or disclosing another User's password.

5.3.3 Password Maintenance

Where possible, passwords should be obscure and a minimum of ten characters in length. For optimum security, passwords should include uppercase, lowercase, numbers, and special characters (i.e., @ - # - $ - &). Where applicable, Users must change their passwords every 90 days. Users who do not change their passwords within the time specified will be locked out of the system.

5.3.4 Passwords Do Not Imply Privacy

As discussed in Section 5.1.1, users should have no expectation of privacy when using the Kaplan Technology assets. The fact that certain users are granted access to password-protected areas of the Kaplan Technology assets does not imply that such users retain any expectation of privacy in material created or received within the Kaplan Technology assets. Kaplan reserves the right, without prior notice, to inspect, examine, audit, read, print, and monitor all data stored on the Kaplan Technology assets.

5.4 Security

5.4.1 System and Network Accessibility

Users may access only those sections of the Kaplan Technology assets to which they have authorisation. A user's ability to gain access to other computers or networks within the Kaplan Technology assets does not imply a right to such access, unless such access is specifically authorised. Users may not browse the Kaplan Technology assets in order to gain access to unauthorised areas.

5.4.2 Network Security

Each user is responsible for ensuring that the use of external public networks, such as the Internet, does not compromise the security of the Kaplan Technology assets. This responsibility includes refraining from any activity that can introduce malicious programs into the Kaplan Technology assets that include but are not restricted to viruses, worms, Trojan horses, e-mail bombs, and backdoor access. For example, users may not use peer-to-peer file sharing services and unauthorised remote access services, such as Kazaa, Gnutella, Morpheus, gotomypc.com, both because such services may violate copyright law and because they permit the introduction of harmful programs into the Kaplan Technology assets.

5.4.3 Security Controls

Users shall not connect to the Kaplan Technology assets by any means other than by those specifically defined by the Divisional IT Staff or Kaplan IT Management. Personally owned devices should not be connected to the Kaplan Technology assets without prior approval. Users may not disable security controls, such as access-management software, virus scanners, passwords, personal firewalls, and audit trails. Users may not attempt to discover security flaws. Tampering with any software protections or restrictions placed on computer applications, files or directories is strictly prohibited.

5.4.4 Monitoring

As discussed in Section 5.1.2, Divisional IT Staff, Kaplan IT Management and limited others, such as members of the Human Resources and Legal departments may monitor a User's use of the Kaplan Technology assets. Monitoring includes, without limitation, reviewing previously viewed Internet sites, material downloaded or uploaded by Users to and from the Internet, and e-mail or instant messages sent and received by Users. Monitoring may be performed at any time, and without prior notice to Kaplan Users. Kaplan may monitor its Users for any reason within its sole discretion, including, but not limited to, preventing or investigating allegations of abuse, assuring compliance with copyright laws, conducting technology audits, conducting internal investigations or complying with legal or regulatory requests for information.

5.4.5 Information Security Policy

Every user, temporary staff, and third party contractors using Kaplan systems and/or data must adhere to the Information Security Policy at all times to ensure safe and secure access to systems and data for business purposes.

5.4.6 Physical Security

Users shall take all reasonable and cautious measures to physically secure hardware items belonging to the Kaplan Technology assets. Users shall not attempt to circumvent any such physical security measures. Laptop Users should lock the laptop or store the laptop in a secure location whenever it is not in use. Mobile device users should ensure that such items are kept secure and that contents are password-protected.

Physical Security

Users shall take all reasonable and cautious measures to physically secure hardware items belonging to the Kaplan Technology assets. Users shall not attempt to circumvent any such physical security measures. Laptop Users should lock the laptop or store the laptop in a secure location whenever it is not in use. Mobile device users should ensure that such items are kept secure and that contents are password-protected.

5.5 Voicemail

5.5.1 Voicemail Setup

If a user has access to the Kaplan Telephone system, he or she should record an appropriate internal and external voicemail greeting and change the voicemail password from the system default to a unique password.

5.5.2 Voicemail Precaution

Confidential Information should not be left as a message under any circumstance.

5.6 Malware, Viruses, Social Engineering and Network Attacks

5.6.1 Virus and Malware Prevention

Viruses have the potential to cause substantial damage to individual computer systems and networks. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the Kaplan Technology assets. To that end, users should not open email or file attachments from unknown sources or disable virus protection software installed on the Kaplan Technology assets. Laptop users should comply with virus definition update announcements as required. All users should report suspected virus activity to Divisional IT Staff or Kaplan IT Management immediately.

5.6.2 Social Engineering

Users should report any instances of impersonation of Kaplan staff or services. Each user is responsible for taking reasonable precautions to ensure that they do not give out their login details, that they confirm the identity of the person they are communicating with and ensure that they identify the correct sender email, URL or application that they are using.

5.6.3 Network Attacks

Users must not knowingly introduce any form of network scanning devices or software onto the Kaplan network. Users are not permitted to alter any network settings without authorisation from Kaplan IT. Any form of network scanning, attempts to penetrate the Kaplan network and deliberate misuse of the Kaplan network will be treated as a Network attack and the user will be held responsible.

5.7 Destruction of Hardware and Software

Kaplan has made significant investments in hardware and software to provide the essential tools necessary to its users. Users must not willfully destroy or otherwise delete any software licensed to or owned by, or any hardware purchased, leased, or otherwise in the possession of Kaplan. Any such damage or destruction shall subject the User to disciplinary action under this policy. Kaplan reserves the right to seek payment through legal action for any damage incurred by the user.

6 Incident Reporting Procedure

6.1 Report All Security Incidents

Users must immediately report any confirmed or suspected security incidents through to the IT Service Desk. Security incidents that must be reported include, but are not limited to, any disclosure of Confidential or Personally Identifiable Information, suspected hacking or computer viruses, unauthorised use of the Kaplan Technology Assets, loss or theft of laptops, or other mobile devices. Please refer to the Incident Response Policy & Procedure for any further information.

6.2 Reporting Paths

You may report such incidents either to the IT Support of your business unit, or to the dedicated data security incident hotline or email address (see 6.2.1 and 6.2.2 below). Please clearly identify that you are reporting a suspected data security incident. Be prepared to give the time and date of the incident, the personnel involved, and a description of the events.

6.2.1 IT Support Numbers

Business Unit	Telephone Number
IT Support Kaplan UK & Ireland	+44 207 920 6844

6.2.2 Dedicated Email Address.

As an alternative, please send an email message to securityandcompliance@kaplan.co.uk. Please include your name, title and business unit, the time and date of the incident, personnel involved, and a description of events, as well as a phone number where you can be reached.

6.2.3 Emergency number out of hours.

In the event of an emergency security incident occurring out of hours please call +44 7983 412 407. Please make sure you leave a number where you can be reached.

7 Exceptions

Exceptions to this policy may be granted through the formal review and approval from the Kaplan IT Management.

8 Cessation of Access

When a user's requirements to use the Kaplan Technology assets ceases:

8.1 Return of Assets

The user must return all Kaplan Technology asset items, such as identification badges, VPN remote access tokens, building access cards, keys, mobile devices, laptops, peripherals (i.e. keyboards, mice, headsets etc.) and any other Kaplan materials. Once the user leaves the business, all the technology assets should be

returned to Kaplan IT, if not then they may be liable for the cost of non-return of the technology assets.

8.2 Revoke Access Rights

A user's access rights to the Kaplan Technology assets, including all User IDs, passwords, VPN remote access, programs, files, intellectual property, or any other mechanisms of access, will be revoked. Thereafter, the user's access to Kaplan's Technology Systems is strictly forbidden.

9 Reference Policy Documents

- Information Security Policy
- Data Protection Policy
- Incident Response Policy & Procedure