INSPIRED EDUCATION HOLDINGS LTD. ("*INSPIRED*")

Acceptable Use Policy

Version 1.0

Date of issue: 7th October 2021

Contents

1. INTRODUCTION

Inspired Acceptable Use Policy ("the Policy") is intended to define which information is authorised to be accessed and used and which data are and are not permitted to use as well as the application of the security measures to protect the confidentiality, integrity and availability of the information processed.

This Policy defines responsibilities for Acceptable Usage of Inspired's resources such as telephony, messaging systems (including email and instant messaging) and the corporate internet connection and Internet services among others.

Information and cyber security in today's workplace, is increasingly important, for example due to the value of data to criminals, laws and regulations protecting data, or the threat of interruption or damage to services or systems. As the first line of defence, colleague's actions whether intentional or accidental, are paramount in protecting the Company's information, including staff, contractors and customer data, services and reputation.

The risks to Inspired, if the controls in this document are not complied with, include but are not limited to:

- Loss or disclosure of data to unauthorised parties.
- Legal or regulatory actions.
- Financial loss resulting from fines, claims or commercial loss.
- Reputational damage.

1.1. Audience

This Policy applies to all Inspired subsidiaries and all employees, employees of third party suppliers and contractors, customers, visitors or third parties who are authorised to access and use the Company's systems (also referred in this Policy as "Users"), working on behalf of the Company who access Inspired systems including outsourced systems, whether on Inspired premises or not.

1.2. Purpose

The purpose of this policy is to detail the acceptable use of the Company IT resources.

The objectives of this Policy are to:

- Provide a safe and secure environment for Users, also considering our customers, colleagues, and Inspired assets whilst supporting Inspired business strategy.
- Explain clearly the responsibilities by setting clear requirements and liabilities for acceptable usage of Inspired computers, Inspired mobile/personally owned devices, systems and data.
- Provide minimum requirements to which a Business Unit must adhere.

The Policy also sets out requirements and controls that aim to:

- Set out clear requirements and responsibilities for acceptable use.
- Helping to protect User's information and Inspired's reputation.

This Policy forms part of the overarching Information Security Policy.

2. SCOPE

2.1. Activities

This policy applies to all Users and to any and all use (and misuse) of Inspired IT resources, including, but not limited, computer equipment, e-mail, instant messaging, the intranet, the internet, telephones, mobile/smart phones or devices (e.g. iPad) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards, computer networks, systems, servers, and software, databases, personal data and information, equipment and devices, email, WiFi, corporate internet connection, any kind of electronic documents, information, intellectual and industrial property as well as other IT systems and other resources as they are added to the Inspired IT environment.

Engaging in activities which are not in accordance with the requirements set out in this Policy or that breaches, laws, regulations or good practice will render Users liable to disciplinary action, which if sufficiently serious or repeated, may lead to dismissal (including summary dismissal due to gross misconduct) or criminal prosecution.

If there is any doubt about the security or acceptability of a particular activity, Users should seek guidance from their line manager immediately.

Inspired may monitor Users' activity where this is required to protect Inspired's information, to meet regulatory or legal obligations or as part of an investigation into suspected misuse.

This Policy is mandatory for all businesses and legal entities across Inspired.

3. GDPR Processing Personal Data in Inspired – Lawful Basis

Under the General Data Protection Regulation (EU) 2016/679 of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) as well as its implementation by Data Protection Act 2018, all processing of personal data within Inspired may only be conducted when there is a lawful basis for doing so, and the processing may only be for the stated purpose and for as long as originally required. The concept of lawful basis according to GDPR, implies e.g. the performance of a contract, to comply with a legal obligation, to protect Inspired legitimate interests or a third party vital interest or to carry out Inspired official tasks or functions, or other specific tasks in the public interest. The lawful basis for each processing element must be duly documented.

All this personal data processed will be kept with the appropriate security measures which ensure the confidentiality, privacy, integrity and availability of such information by applying the required security measures.

Inspired employees and third-parties must understand the legal basis of each processing element and ensure that the processing is conducted according to the agreed and defined legal basis.

4. MANDATORY REQUIREMENTS

4.1. Acceptable Use Management – Accountabilities and Responsibilities

Clear accountability for Acceptable Use must exist at all levels and across all areas of Inspired.

IT resources are available and used for productive business of Inspired. To ensure the IT resources are used appropriately, Users are prohibited from engaging in any activity with IT resources that may jeopardise or are contrary to appropriate use. In particular, the transmittal, retrieval, or storage of information that is inappropriate for the workplace is not permitted while at work or with Inspired resources. Prohibited use includes but is not limited to content involving nudity, violence, illegal drugs, sex, or gambling, or involves discriminatory, harassing, disturbing, obscene or pornographic material. In addition to these guidelines, Users should use common sense and consideration for others in deciding which content is appropriate for the workplace.

4.2. Technology Provider (IT)

The IT Department will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

4.2.1. All Users

Inspired's messaging systems, internet facilities and telephony are provided only for business purposes. Users may use them for limited and occasional personal use in accordance with the requirements of this Policy.

Inform your line manager and/or HR immediately if you receive or access illegal, offensive or obscene material:

- From a telephone call, in a text, email or any instant message.
- On an Internet site.
- Unsolicited receipt or accidental access is not a disciplinary offence but must be immediately reported.

4.3. Equipment Security and Passwords

Users are responsible for the security of the equipment allocated to/used by them and must not allow it to be used by anyone other than in accordance with this policy or as specifically authorised in writing by their line manager.

Users given access to the e-mail system, intranet, internet or any online resource, are responsible for the security of their computers. Users without authorisation should only be allowed to use computers under supervision and as agreed with their line manager.

Users must lock, log off or shut the system down when leaving a computer unattended. Laptops must be turned off overnight and during transit.

Securely store equipment, paper and other media away when not in use.

Desktop PCs and cabling for telephones or computer equipment should never be moved or tampered with. Requests for such changes should be made to the IT Department.

Passwords are unique to each user and may be changed on a random basis enforced by IT. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Head of Infrastructure and Data Security

4.3.1. Passwords must adhere to the following rules:

- Minimum of 8 characters in length
- Contain both numeric and alphabetic characters (one must be a capital letter)
- The password should be periodically changed (every 3 months, at least)

Users must not use easily guessable words or number/letter sequences for passwords, e.g. dictionary words, family member or pet names, 1234, qwerty etc. Passwords must be kept secure they must not be shared. Authorised users are responsible for the security of their passwords and accounts. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

For the avoidance of doubt, on the termination of employment (for any reason) Users must return any equipment, key fobs or cards and they will have no rights of access to the Inspired systems.

Users who have been issued with a laptop, mobile/smart phone or device must ensure that it is kept secure at all times, especially when travelling.

Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Users should also be aware that when using equipment away from the workplace, documents may be read by third parties (for example, passengers on public transport) and must take all reasonable steps to avoid this.

Inspired has a separate Mobile Devices Policy that sets out the minimum requirements for the secure management of information accessed or held on Mobile and Personal Devices.

All Users issued with laptops, mobile/smart phones or devices must read and strictly adhere to this Policy.

Third party and personally owned devices must only connect to Inspired's corporate network if they meet the requirements stipulated in the Inspired Mobile Devices Policy.

4.4. Systems and Data Security

Users should not delete, destroy, modify or interfere with any part of computer equipment, systems or data (e.g. anti-virus software or firewalls), including programs, information, data, any equipment or network or any software used which could have the effect of harming our business or exposing it to risk.

Users should not download or install software from external sources without authorisation from the Head of Infrastructure and Data Security. This includes (but is not limited to) software programs, instant messaging programs, screensavers, photos, video clips and music files.

No device or equipment should be attached to the Inspired Systems without the prior approval of the IT Department. This includes (but is not limited to) any USB flash drive or similar device, mobile/smart phone or device or telephone. It also includes (but is not limited to) use of the USB port, infra-red connection port or any other port on any device connected or having access to Company Systems.

Multi factor authentication for all remote access must be utilised. i.e. originating from outside the entity's network. This includes both Inspired User and administrator access, and third-party access for supporting and maintenance.

In addition to a unique ID two of the three following methods are required to authenticate all users, where appropriate and applicable:

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a biometric.

Using one of the above methods twice, e.g. using two separate passwords to gain access, is not acceptable.

Inspired monitors all e-mails passing through its system for viruses. Users should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious. The user's Line Manager should be informed immediately if a suspected virus is received. Inspired reserves the right to block access to attachments to e-mails for the purpose of effective use of the Systems and for compliance with this policy. Inspired also reserves the right not to transmit any e-mail message.

Users should not attempt to gain access to restricted areas of the network, or to any password-protected information. Requests for amended access rights should be directed to the Line Manager and Head of Infrastructure and Data Security.

Users using laptops or Wi-Fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT Department from time to time against importing viruses or compromising the security of the Systems. Systems contain information which is confidential to Inspired business and/or which is subject to data protection legislation.

Users must destroy paper and other media in line with local procedures for approved destruction purposes. Only use bins which are specifically designated for this purpose. Users must never dispose of paper in general or domestic waste.

Users must clear desks, printers, photocopiers, fax machines, meeting rooms and white boards at the end of each business day.

4.5. Confidentiality and Copyright Protection

Users shall not modify, reproduce, duplicate, copy, re-sell or distribute for any commercial/personal purpose any materials or content on Inspired systems/applications without the prior written consent of Inspired or the copyright owner. In particular, it is up to Users to check the terms and conditions of any license for the use of the software or information and to abide by them. Software and information provided by Inspired may only be used in the course of your duties as an employee of Inspired.

Users must abide by all of the licensing agreements for software entered into by Inspired with other parties.

4.5.1. E-mail (including Instant Messaging) Etiquette and Content

E-mail, instant messaging and the intranet is a vital business tool but an informal means of communication and should be used with great care, accuracy and discipline. Users who use the

Inspired's e-mail services are expected to do so responsibly and they must comply with all applicable laws as well as this policy.

Users should always consider if e-mail/instant messaging is the appropriate means for a particular communication and correspondence sent by e-mail/instant messaging should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Users must be always sure that they send the e-mail to the correct receiver. An organisation standard disclaimer with the corresponding confidentiality clause is automatically added to all outgoing email.

Users should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out of office response when away from the office.

Users should take care with the content of e-mail/instant messaging, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Users should assume that e-mail/instant messages may be read by others and not include anything which would offend or embarrass any reader, Inspired or themselves, if it found its way into the public domain.

E-mail/instant messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail/instant message cannot be recovered for the purposes of disclosure. All e-mail/instant messages should be treated as potentially retrievable, either from the main server or using specialist software.

Users should not:

- Send or forward e-mails/instant messages that contain anything which may be considered by anyone to be offensive, abusive, obscene, harassing, derogatory, defamatory or discriminatory, including discriminatory to others based on their race, sexual orientation, age, disability or religious or political beliefs.
- Send or forward private e-mails at work which they would not want a third party to read.
- Use personal email accounts for sending or receiving non-public Inspired information.
- Send or forward chain mail, junk mail, cartoons, jokes or gossip.
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter.
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this.
- Send messages from another User's computer or under an assumed name unless specifically authorised.
- Send confidential messages via e-mail/instant messaging or the internet, or by other means of external communication which are known not to be secure.

Any User that receives any of the above from another User via e-mail should inform their line manager or the HR Department.

Users who receive a wrongly-delivered e-mail should return it to the sender. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

If you have any doubts over this e-mail policy, please contact your line manager before dealing with an email.

4.5.2. Video Conferencing

Use of video conferring is for business purposes only. Users are required to act professionally and respectfully at all times. Video conferences are required to be treated like a normal meeting with a customer or any other User. No foul language or obscene images should be used. If a User's screen is being shared, such User is required to make sure that no confidential data or private information of other Users or customers as well as Inspired confidential information is displayed.

Users are required to always use the highest security settings during all video conferences.

4.6. Use of the Internet

Internet is to be used for business purposes only and usage will always be monitored by Inspired. When a website is visited, devices such as cookies may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind displaying the material described in the "inappropriate use of equipment or systems" section such a marker could be a source of embarrassment to the visitor and Inspired, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website.

Users should not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that Inspired software has accessed the page, or the file might be a source of embarrassment if made public, then viewing it will be a breach of this policy. Such actions may also, in certain circumstances, amount to a disciplinary and/or criminal offence if, for example, the material is pornographic in nature.

4.7. Personal Use of Systems

Inspired permits the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be abused or overused and Inspired reserves the right to withdraw its permission at any time.

The following conditions must be met for personal usage to continue:

- Use must be minimal
- Personal e-mails must be labelled "personal" in the subject header.
- Use must not interfere with business or office commitments.
- Use must not commit Inspired to any costs.
- Use must comply with Inspired policies including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure (and all sections of this Acceptable Use Policy).

4.8. Use of Social Media

Inspired has a separate Social Media Policy that sets out the Inspired's requirements for a robust social media approach to effectively manage social media risks.

Social media refers to the posting and sharing of content in digital communities and networks.

Social media accounts are intended to be used solely for business purposes. It includes a wide range of websites and "apps" which allow users to interact with others. This Social Media Policy applies to all social media including Facebook, Twitter, LinkedIn, Pinterest, Tumblr, Flickr, Google+, Instagram and any other social media or similar platform or associated tools. It includes any comments you make or leave on blogs or Facebook pages, edits to wikis, responses to Tweets, postings on message boards or forums, opinions on online polls and any other activity that might reasonably be considered to fall within the term "Social Media".

All colleagues must read and strictly adhere to this Policy at all times.

4.9. Use of Mobile Devices for Business Purposes

Inspired has a separate Mobile Devices Policy that sets out the minimum requirements for the secure management of information accessed or held on Mobile Devices, authorised to connect to the Corporate Network. The mobile devices that are property of Inspired are intended to be used for business purposes only and will be monitored and controlled by Inspired at all times.

All relevant colleagues must read and strictly adhere to this Policy at all times.

4.10. Telephony

Telephones may only be used in accordance with this policy. Telephones are provided to enable Inspired employees to carry out their duties and for customers, third party suppliers and other business contacts to contact Inspired.

A nuisance call is defined by law as "…. *a message or other matter that is grossly offensive or of an indecent, obscene or menacing character*". A nuisance call can also be a caller who makes persistent silent calls. Whatever the nature of the call, Inspired does not want any of its employees, customers, suppliers or other business contacts to suffer the distress and inconvenience this type of call causes.

If any User becomes a victim of a nuisance call at work, they should report it to the HR Department who will inform them of the process to follow; this may include the colleague recording details to be passed on to the police. If any User receives nuisance calls from another User, they should contact their line manager and/or the HR Department.

4.11. Monitoring of Use of Systems

Inspired systems/applications, including computers, enable it to monitor the access and use to telephone (and record calls in some instances), e-mail, instant messaging, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in its role as an employer, use of Inspired Systems including the telephone and computer systems, and any personal use of them, is continually monitored. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes. Normally, monitoring the

use will be carried out where there is suspected criminal activity or malpractice such as theft or fraud by Users.

On the grounds of the GDPR and Data Protection Act 2018, Inspired can control or monitor the use of the systems on a lawful basis of legitimate interest on monitoring workplace. This purpose cannot be overridden by the interests or fundamental rights of the employees but must be proportional, justified and limited, always respecting User's privacy.

Users should have no expectation of privacy in work, particularly in connection with the use of IT and Inspired devices that are provided to be used only for business purposes. Inspired will communicate to Users this monitoring purpose through different ways such as an e-mail/internet policies, its data protection policy or employee privacy notice.

CCTV systems monitor the interior and exterior of our buildings 24 hours a day. This data is recorded.

Inspired reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

- To monitor whether the use of the e-mail/instant messaging system or the internet is legitimate and in accordance with this policy
- To find lost messages or to retrieve messages lost due to computer failure
- To assist in the investigation of wrongful acts
- To comply with any legal obligation.

4.12. Inappropriate Use of Equipment and Systems

Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with the Company's rules, policies and procedures (including but not limited to this policy, the Equal Opportunities Policy, Data Protection Policy and the Disciplinary Procedure).

Misuse, excessive use, inappropriate use or abuse of Company telephone or e-mail/instant messaging systems or internet is in breach of this policy will be dealt with under the Company's Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to the Company, its colleagues or its clients.
- A false and defamatory statement about any person or organisation.
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others.
- Confidential information about the Company or any of its employees or clients (when accessed by an employee who has no such authority to do so).
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee that made the statement or for the organisation.
- Material in breach of copyright.

Causing security breaches or disruptions of internet communications is strictly prohibited. Security breaches include, without limitation, accessing data not intended for the User in question, or logging onto a server or account that the User is not expressly authorised to access.

When reference is made to, "*disruption*" it shall include, without limitation, deliberate attempts to overload a service, attempts to crash a host, the introduction of any malicious code, such as computer viruses or "*trojans*", onto any part of the Inspired's computer network.

4.13. Use of office materials and equipment

All office materials, furnishings and supplies provided to Users are property of Inspired and are to be used for business purposes only. Generic materials, such as pens, blank paper and the like, may be freely accessed but are not to be removed from Inspired without prior consent. Specific materials such as letterheads must and will have restricted access and are not to be removed from Inspired without prior consent.

Users are not allowed to place any material belonging to Inspired, including software or any internal information, on any publicly accessible internal or external website without the prior written approval of the Inspired CEO.

5. MANDATORY REQUIREMENTS

5.1. Training

All Users, including contractors, must complete the Information Security and Data Protection training (includes an Acceptable Use element), within eight (8) weeks of joining Inspired and then annually.

5.1. Non-Compliance

5.1.1. Waivers

Waiver requests must be made to the IT Steering Group for approval where there are exceptional reasons for non-compliance with this Policy and must be time limited and tracked.

5.1.2. Violation

Any violation of this Policy must be escalated in line with HR guidelines (Employee abuse/misuse).

All violations must be discussed at the next IT Steering Group meeting.

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Inspired's applicable disciplinary code, and may include the termination of employment contract, or cancellation or termination of contractual or commercial relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Inspired's disciplinary code and procedures.

6. RELATED POLICIES AND GOVERNANCE DOCUMENTS

Information Security Policy	Sets out the Company's requirements for a robust Information Security approach to protect, preserve and manage the confidentiality, integrity and availability of Company information and all supporting processes, applications and systems.
Social Media Policy	Sets out the Company's requirements for a robust social media approach to effectively manage social media risks.
Mobile Devices Policy	Describes the minimum requirements for the secure management of information accessed or held on Mobile Devices, authorised to connect to the Corporate Network.

The policy will be reviewed and approved on an annual basis by the relevant departments or in the event of significant change to business or regulatory environments.

Last version was issued in October, 2021

7. DOCUMENT VERSION CONTROL

Version number	Author	Approval Date	Effective Date	Status/comments
V0.1	Jason French	DRAFT		Initial Draft released by Cyber Security Project Manager following review by Infrastructure SME and Head of Infrastructure and Data Security
V0.2	Jason French	DRAFT		Updated Following HR review
V0.3	Patricia Sarrais	DRAFT		Group DPO and Legal advisor review amendments
V0.4	Jason French	DRAFT		IT Roles and responsibilities confirmed following confirmation from Head of Infrastructure and Data Security
V1.0	Jason French	Approved	07/10/21	Review and approval by CIO. Amendment to roles and responsibilities