Objective

The purpose of this policy is to outline the acceptable use of information technology at Pearson. These rules are in place to protect employees, Pearson and our customers. Inappropriate use exposes every employee and Pearson to risks including virus/malware based attacks, network systems and services being compromised, legal issues, and breaches of trust with our learners and customers.

Overview

Our aim is to establish an Acceptable Use policy that is consistent with, and promotes, our core values: to be brave, imaginative, decent and accountable to our stakeholders and each other. The Chief Information Security Office is committed to protecting Pearson users* and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a company wide effort involving the participation and support of every Pearson user and affiliate who deals with information and/or information systems. It is the responsibility of every information technology user to read and understand these policies, and to conduct their activities accordingly.

Scope

This policy applies to the use of information, in any medium, electronic and computing devices, and network resources to conduct Pearson business or interact with internal networks and business systems, whether owned or leased by Pearson, the user, or a third party. All users at Pearson and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Pearson policies and standards, and local laws and regulation. This policy applies to all users at Pearson including all personnel affiliated with third parties. This policy applies to all information technology that is owned or leased by Pearson, or used to conduct Pearson business including personally owned devices.

Policy

General Use and Ownership

a. Pearson proprietary (information classified as DCL2-DCL4**) information, whether in hard copy form or stored on electronic and computing devices, whether owned or leased by Pearson, the user or a third party, remains the sole property of Pearson or its owner. You must ensure through legal or technical means that proprietary information is protected in accordance with all Pearson policies and regulatory requirements.

b. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Pearson proprietary information. All users will be aware of their responsibilities to report known or suspected information security events and
Acceptable Use Policy

security weaknesses as quickly as possible. Reports should be submitted to
the Security Operations Center at soc@pearson.com, or +44(0)207 010 5525. They may also be reported to management, the Corporate Help Desk, through
the SOS button on myCloud/myHelp, or any member of the Office of the Chief
Information Security Officer.

c. Users may access, use or share Pearson proprietary information only to the
extent it is authorized and necessary to fulfill your assigned job duties.
d. Pearson data must be stored and processed on systems approved by Pearson
business and IT management. No user is authorized to engage or utilize any
other systems, either Pearson owned or Cloud based, individually or as a
business.
e. Users are responsible for exercising good judgment regarding appropriate and
reasonable use of the Pearson intranet and Pearson-provided/paid devices to
include smartphones, tablets, and laptops. Occasional, limited personal use
(ie: web browsing, checking personal email, etc.) during assigned work hours
is allowed if it does not violate any Pearson policy or local law. Usage for any
other personal activities, private or commercial, is expressly prohibited. As
allowed by local law, Pearson may track usage for excessive personal use and
reserves the right to revoke devices where abuse is occurring. Please check
with your department supervisor or manager for specifics on what constitutes
acceptable personal use.
f. For security and network maintenance purposes, authorized individuals within
Pearson may monitor equipment, systems and network traffic at any time, per
the authority of the office of the Chief Information Security Officer.
g. In accordance with local laws, Pearson reserves the right to audit networks
and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

h. All mobile and computing devices authorized to connect to the internal
network must comply with all policies governing secure configuration and
access control.
i. Users are responsible for exercising good judgment regarding appropriate and
reasonable use of Pearson-provided/paid devices to include smartphones,
tables, and laptops.
j. System level and user level passwords must comply with the Password Policy
and be changed every 60 days without exception.
k. Providing access to another user, either deliberately or through failure to
secure its access, is prohibited.
l. All devices used to access Pearson IT systems must be secured with a
password-protected screensaver with the automatic activation feature set to
15 minutes or less where available. Wearable devices without this function
must be set to lock when the device is not on the wrist or when they are out of
contact with the associated smartphone. You must lock the screen or log off
when the device is unattended.
m. Postings by users from a Pearson email address to newsgroups should contain
a disclaimer stating that the opinions expressed are strictly their own and not
necessarily those of Pearson, unless posting is in the course of business
duties.
n. Users must use extreme caution when opening email attachments received from unknown senders, which may contain malware. If the user is not sure of the source, the email should be deleted. Users may contact the Help Desk or their Desk Side support team for assistance.

o. When not being used, all hardcopy and electronic storage media containing sensitive information must be locked in file cabinets, desks, safes, or other secure locations.

Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a Pearson user, utilizing Pearson owned resources or personally owned resources, authorized to engage in any activity that is illegal under local, state, federal or international law.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

p. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Pearson, or use of open source software product without Pearson’s consent.

q. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other sources, music, videos, and the installation of any software for which Pearson does not have an active license is strictly prohibited.

r. Accessing Pearson data, a server, or an account for any purpose other than conducting Pearson business, even if you have authorized access, is prohibited.

s. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

t. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

u. Copying unencrypted, sensitive (DCL2-4) Pearson data to an unencrypted removable storage medium.
v. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done remotely.

w. Using a Pearson computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

x. Accessing, downloading, storing, sharing or linking to any prohibited content, including, but not limited to images of children that include nudity or erotic posing. Images of children involved in any sexual activity with adults or other children, this would include images involving sadism and/or bestiality.

y. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

z. Port scanning or security scanning is expressly prohibited unless prior notification is made to, and approval is received from, the office of the Chief Information Security Officer.

aa. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

bb. Circumventing user authentication or security of any host, network or account.

c. Introducing honeypots, honeynets, or similar technology on the Pearson network.

dd. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

e. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/intranet/ extranet.

ff. Modifying Pearson-provided technology in any way intended to circumvent security measures.

gg. Providing information about, or lists of, Pearson users, learners, stakeholders or others to parties outside Pearson without their express written consent and permission from Pearson Legal.

hh. Using a non-Pearson-assigned cloud service or other unauthorized medium for storage of Pearson data including forwarding Pearson information to a personal system or email address.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever users state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

ii. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). **NOTE** – Businesses that utilize email for solicitation
related to product development, customer or anonymous feedback, or other legitimate Pearson sanctioned activities must assure they are in compliance with all national and state regulatory restrictions (ie: CAN-SPAM Act, etc ...) prior to initiation of those solicitations. Consult Pearson Legal and/or CISO for guidance.

jj. Any form of harassment via email, telephone, texting, whether through language, frequency, or size of messages.

kk. Unauthorized use, or forging, of email header information.

ll. Sending solicitation emails from any email address with the intent to harass or to collect replies.

mm. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

nn. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

oo. The system should not be used for discussion of potential or actual legal disputes with anyone other than Pearson Legal Counsel. Users should bring any such issues promptly to the attention of Pearson Legal Counsel. Unless and until Pearson Legal Counsel asks the end user to do so, the system should not be used to create new documents or summaries of the facts or events of the dispute. Users should also not delete any messages or other documents that the user has already sent or received about a legal matter unless Pearson Legal Counsel advises the user to do so.

pp. The Pearson Legal Department may send notices to System Administrators and end users requiring that emails on particular subjects, or to or from particular users, be saved and/or copied onto removable media to be saved until further notice, or forwarded to the Legal Department. If this happens, the Legal Department’s notice will supersede any policies or procedures that are in place regarding the automatic or manual destruction of emails.

qq. All users that are provided with a Pearson email account (name@pearson.com) MUST use that account for the conduct of all Pearson business. Users not provided a Pearson email account may use personal email accounts for general communication for Pearson business, but MUST NOT share or transmit any protected, sensitive, or confidential Pearson, customer, partner, or vendor information through those accounts.

Use of Non-Pearson Social Media

rr. Use of Social Media, whether using Pearson’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Use of Pearson’s systems to engage in the use of social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Pearson’s policy, is not detrimental to Pearson’s best interests, and does not interfere with an user's regular work duties. Use of Social Media from Pearson’s systems is also subject to monitoring.

Users are prohibited from posting images of, or comments about learners without their consent.

ss. Users are prohibited from revealing any Pearson confidential or proprietary information, trade secrets, marketing plans, or any other material classified as DCL2, DCL3 or DCL4 under Pearson’s Data Classification and Labeling policy.
when engaged in the use of social media. Users assume any and all risk associated with the use of social media.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Pearson’s trademarks, logos and any other Pearson intellectual property may also not be used in connection with any social media activity.

See the Pearson Social Media Security Policy for additional controls and requirements. (https://neo.pearson.com/docs/DOC-375320)

Additional Pearson Policies and Standards

Additional Pearson policies all users must be aware of, and comply with, are available on the CISO-Global Information Security site at https://neo.pearson.com/groups/global-infosec

Sanctions
Pearson will employ logical and technical methods to monitor and audit for violations of information security policies and internal controls. User who violate this policy may face disciplinary action up to, and including, termination of employment. Individuals, who are not employees, found to be in violation of this policy are subject to having their access revoked and their contract terminated.

Implementation
Technical teams responsible for the configuration and maintenance of Pearson information systems and applications are responsible for implementing all controls required for the secure operation and protection of those assets. They are authorized to identify and implement all controls necessary for the security and safe operation of those systems that are not explicitly stated in policy or standards. All such controls shall be documented and raised to CISO as suggested changes, and shall be reviewed and considered for documentation to be added to the next revision of the appropriate policy or standard.

This policy has controls that are designed to support, ensure and evidence Pearson legal compliance including, but not limited to, GDPR, SOX, HIPAA, due diligence and duty of care to all of Pearson's customers and stakeholders.

Responsibility

Pearson
Pearson will employ best practices and all other allowable means to enforce the provisions of this policy to ensure the Confidentiality, Integrity and Availability of Pearson company assets.

Information Security Officer
The Information Security Officer (ISO) has direct responsibility for Pearson Security Policy compliance, for providing guidance on best business security practices, and managing the Exception Process.
Business Management
All business managers are directly responsible for implementing all Pearson policies and controls within their business areas, and for awareness and adherence by their staff.

Personnel
All personnel will be aware of Pearson policies, and act in a manner that complies with, and supports, this policy both in content and in spirit, and will report all suspected and known violations.

Exception Process
Any exception to the application of this policy, or individual policy statements within, or any supporting policies, requires prior written approval from the Office of the CISO. All exception requests must be evaluated and approved by the designated level of management of the requesting organization, with a clear statement of their acceptance of any residual risk created through the exemption. The Exception Process and required documents are at https://neo.pearson.com/docs/DOC-586645

Questions about this or any other Information Security Policy should be referred to InfoSecGRC@Pearson.com

Document Approval and Ownership
The Chief Information Security Officer is the owner of this document and is responsible for ensuring that it is reviewed annually. This policy was approved by the Pearson Executive Security Governance Board, and is issued on a version-controlled basis under the authority of the Chief Information Security Officer.

Chief Information Security Officer: Rod Wallace
Approval Date: May 1, 2015

Change history
<table>
<thead>
<tr>
<th>Version</th>
<th>Date Issued</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>May 1, 2015</td>
<td>Original Version</td>
</tr>
<tr>
<td>1.0</td>
<td>April 28, 2016</td>
<td>Reviewed and Re-authorized</td>
</tr>
<tr>
<td>1.0</td>
<td>April 28, 2017</td>
<td>Reviewed and Re-authorized</td>
</tr>
<tr>
<td>1.1</td>
<td>January 5, 2018</td>
<td>Clarification of personal use, Paragraph e.</td>
</tr>
<tr>
<td>2.0</td>
<td>September 19, 2018</td>
<td>Addition of Implementation section, edits to Responsibility Section</td>
</tr>
</tbody>
</table>
Acceptable Use Policy

Definitions

* "User" – User means any employee, contractor, consultant, temporary workers and other individuals having access to the Pearson network/systems.

**This standard defines the specific security controls that must be employed to protect data at each of the following DCL levels, as defined in the Data Classification Policy at [https://neo.pearson.com/docs/DOC-592807](https://neo.pearson.com/docs/DOC-592807):

- DCL1 – Public---May also be referred to as “Unclassified”
- DCL2 - Internal Use Only---May be referred to as “Internal” or “Proprietary”
- DCL3 - Confidential---May also be referred to as “Company Confidential” “Customer Confidential” “Employee Confidential”
- DCL4 - Restricted---May also be referred to as “Highly Confidential” or “Highly Restricted”