



# JRIS Technology Use Policy

سياسة استخدام التكنولوجيا في مدرسة جدة الراقية العالمية

## Policy for Using School Systems, Network, Internet, and Email

1. The provisions of these regulations shall apply to all school staff, faculty, staff, and students.
2. These regulations include the entire school network, whether wired or wireless, its applications, the Internet, e-mail services, or any way through which the school network is connected.
3. The school shall allow staff access to the Internet to assist them in carrying out their duties. Network shall be used only for purposes related to delivering work required and shall not be used for other purposes.
4. For Internet and e-mail service, the user must have a username name, and password. The use of the Internet without a user name is prohibited in any way.
5. The school has the right to monitor and record every activity of the user on the Internet, registerer it, and issue reports in this regard. The school has the right to stop the user when not in compliance with this policy.
6. The school disclaims responsibility for any material accessed via the Internet, any damage, to it, and any other consequences of using the Internet. This includes data that is retrieved during a network connection.
7. The school has the right to block any site or group of sites as needed.
8. E-mail, user, name, and PIN are the responsibility of the user only he/she/ she is fully responsible for any misuse recorded on it.
9. In the event of resignation, the school will be suspending all accounts immediately, and after a full month will be deleting all accounts unless in some exceptional cases and under the direction and approval of the concerned department.

10. The school's official e-mail shall be used for official correspondence and no other e-mail shall be used.

11. Internet connection throughout the school is not to be used for any illegal purposes. Using the internet must not produce or cause conflict with known public morals.

12. It is prohibited to attempt to deceive or corrupt security measures on school network resources or any other system connected to the Internet or accessible via the Internet. If so, the employee is liable for legal accountability.

13. It is forbidden to create or use illegal copies of copyrighted material, store such copies on school equipment, or transmit them through the school network. Illegal use is prohibited, such as: sending, downloading, or publishing any material that violates the laws of the Kingdom of Saudi Arabia or is contrary to Islamic morals or teachings or any of the rules and regulations.

14. Users of a school service or network should not use the service in a way that badly affects other users, the network, devices, and network security, especially the spreading of computer viruses.

15. Users of a school service or network who identify or notice a suspected security problem should immediately contact the IT and Network department.

16. It is forbidden to add, delete or modify network information in an attempt to deceive or mislead any person, either a member of the school or outside it. Impersonating a person with false information through the school network is forbidden under any circumstances and for any reason.

17. It is forbidden to use the school network and email system to send unwanted emails as "advertising emails". Assisting others in spreading these unwanted emails is also forbidden.

18. Creating services that allow others to access your computer is prohibited. Attempting to access others' accounts, or attempting to breach security measures at the school is strictly prohibited.

19. Personal or work-related information may not be obtained or attempted to be obtained by third parties without the knowledge or agreement of the persons concerned. Taking the personal information

of a school official and sending it to another party without his knowledge and consent is strictly prohibited.

20. It is prohibited to give Internet service provided by the school to a third party without consulting and taking approval from the Information Technology Center.

21. Any activity that may adversely affect the ability of others to use the Internet services provided by the school is strictly prohibited.

22. Interference or disruption of networks of other users or network devices is prohibited. The user must take care of the security of the network. The student, faculty, and employee must not allow others to use their networks for illegal or inappropriate work. The user must maintain his or her network password so that no third-party imposition is allowed.

23. Long or drained connections or multiple sign-in are prohibited. The use of a personal account for the depleted use of resources is prohibited. The IT Center reserves the right to cancel any connection that is deemed to be depleted or inactive for a long time.

24. Internet can only be accessed using the school's Internet. You may not use any other method of accessing the Internet within the school. Commercial Internet connection and connecting it to the school network without the knowledge of the IT Center and obtaining written permission is strictly prohibited.

25. It is forbidden to download all types of programs from the Internet and install them on the school's computers. If you need to download work-related programs, please contact the Technical Support Unit at the IT Center.

26. For more prevention & protection against viruses, it is forbidden to use flash drives and optical discs for the safety of the network and to preserve the privacy of information.

27. The use of computers and peripherals connected to the server shall be within official working time. (In case of off-duty hours, the names of employees should be submitted to the Information Technology Center).

28. It is forbidden to falsify your identity on the Internet as another person. (Impersonating the Internet.)

29. It is forbidden to use the Internet in a way that delays the use of others, such as spreading viruses or sending service block messages.

30. It is forbidden to enter suspicious sites to hack and download hacking or spyware on school or personal computers

31. It is forbidden to penetrate sites or devices inside or outside the school network using any devices or any means whatsoever with or without intention.

32. The school has the right to take the measures it deems appropriate against those who violate these regulations

33. The school retains the amendment to this policy when necessary.

Upon signing, this policy is considered binding.

Agree (\_\_\_\_)

Name: \_\_\_\_\_ Occupation: \_\_\_\_\_

Disagree (\_\_\_\_)

Signature: \_\_\_\_\_

## سياسة استخدام أنظمة وشبكة المدرسة و الإنترنت و البريد الإلكتروني

1. تسري أحكام هذه الضوابط على جميع منسوبي المدرسة وهم الهيئة التدريسية، الموظفون والطلاب.
2. تشمل هذه الضوابط شبكة المدرسة كاملة سواء أكانت سلكية أم لاسلكية وتطبيقاتها و الإنترنت و البريد الإلكتروني أو أي طريقه يتم الاتصال عن طريقها بشبكة المدرسة
3. تتيح المدرسة للموظفين الوصول إلى الإنترنت لمساعدتهم في القيام بواجباتهم المناطة بهم والمتعلقة بالمدرسة ويجب أن يتم استخدامها لأغراض متعلقة بوظائفهم و لا تستخدم لأغراض أخرى لا تمت إلى العمل بصلة.
4. للحصول على خدمة الإنترنت و البريد الإلكتروني يجب أن يكون المستخدم حاصلاً على اسم مستخدم معروف و كلمة مرور. و يمنع استخدام الإنترنت بدون اسم مستخدم بأي شكل من الأشكال.
5. يحق للمدرسة أن تقوم بمراقبة ورصد كل نشاط يقوم به المستخدم على الإنترنت وتسجيله وإصدار تقارير بهذا الخصوص وإيقاف المستخدم عند عدم الإلتزام بهذه السياسة.
6. تخلي المدرسة مسؤوليتها عن أي مواد يتم الوصول إليها عبر الإنترنت، و عن أي تلف يتم التعرض له وأي عواقب أخرى لاستخدام الإنترنت. وهذا يتضمن البيانات التي يتم استرجاعها أثناء الاتصال بالشبكة.
7. للمدرسة الحق في حجب أي موقع أو مجموعة مواقع حسب ماتقتضيه الحاجة.
8. البريد الإلكتروني و اسم المستخدم و الرقم السري مسؤولية المستخدم الخاص به فقط و هو / هي مسئول بالكامل عن أي سوء إستخدام يسجل عليه.
9. في حالة استقالة أو خروج المستخدم من المدرسة سوف يتم تعطيل جميع حساباته مباشرة، وبعدها بشهر كامل يتم حذف حساباته إلا في حالات استثنائية و بتوجيه من قبل الإدارة المعنية.
10. يستخدم البريد الإلكتروني الرسمي للمدرسة في المراسلات الرسمية و يمنع استخدام أي بريد الإلكتروني آخر.
11. لا يستخدم الاتصال بالإنترنت من خلال المدرسة لأي أغراض غير قانونية أو غير شرعية أو تتعارض مع الآداب العامة.
12. تمنع محاولة خداع أو إفساد إجراءات الأمن على موارد شبكة المدرسة أو أي نظام آخر متصل بالإنترنت أو يمكن الوصول إليه من خلال الإنترنت. و إذا ثبت ذلك فإن الموظف يكون عرضة للمساءلة القانونية.
13. يمنع إنشاء نسخ غير قانونية من المواد المحمية بحقوق نشر أو استخدامها أو تخزين مثل هذه النسخ على أجهزة المدرسة أو إرسالها عبر شبكة المدرسة. كما يمنع الاستخدام غير القانوني مثل : إرسال أو تحميل أو نشر أي مادة تنتهك القوانين المعمول بها في المملكة العربية السعودية أو منافية للأخلاق أو التعاليم الإسلامية أو أي من القواعد والأنظمة.
14. على مستخدمي خدمة أو شبكة المدرسة عدم استخدام الخدمة بشكل يؤثر سلباً على المستخدمين الآخرين أو على التشغيل الاعتيادي للأجهزة والشبكات ، بما في ذلك تحميل فيروسات الحاسب الآلي
15. يجب على مستخدمي خدمة أو شبكة المدرسة الذين يتعرفون على أو يلاحظون مشكلة أمنية فعلية أو مشتبه بها، الاتصال فوراً بقسم الشبكة والتشغيل بمركز تقنية المعلومات.

16. يمنع إضافة أو حذف أو تعديل معلومات الشبكة في محاولة للخداع أو التضليل .يمنع محاولة انتحال شخصية ما عن طريق معلومات مزورة عن طريق شبكة المدرسة.
17. يمنع استخدام الانترنت لإرسال رسائل إلكترونية غير مرغوب فيها. كذلك يمنع أي نشاط يسهل من عملية إرسال تلك الرسائل سواء أكان محتوى الرسالة تجارياً أم غير ذلك.
18. يمنع إنشاء خدمات تسمح للآخرين الوصول إلى جهازك أو في محاولة الوصول إلى حسابات الآخرين أو محاولة اختراق الإجراءات الأمنية للمدرسة.
19. يمنع الحصول على معلومات شخصية أو معلومات تخص العمل أو محاولة الحصول عليها لأطراف ثالثة من دون علم الأشخاص المعنيين أو موافقتهم، كأخذ معلومات شخصية لمسؤول بالمدرسة وإرسالها لطرف آخر من دون علمه و موافقته على ذلك.
20. يمنع إعادة إتاحة خدمة الإنترنت المقدمة من قبل المدرسة لطرف خارجي من دون الحصول على ترخيص من مركز تقنية المعلومات بذلك.
21. يمنع أي نشاط قد يؤثر سلباً على قدرة الآخرين في استخدام خدمات الانترنت المقدمة من المدرسة.
22. يحظر التدخل أو تعطيل شبكات مستخدمين آخرين أو أجهزة الشبكات. وعلى المستخدم الحرص على أمان الشبكة. ويجب على الطالب، وعضو هيئة التدريس، والموظف عدم السماح للآخرين باستخدام الشبكات الخاصة بهم لأعمال غير قانونية أو غير لائقة. على المستخدم الحفاظ على الشبكة الخاصة به بحيث لا يسمح باقتحام طرف ثالث لها.
23. تمنع الاتصالات الطويلة أو المستنزفة أو تسجيل الدخول المتعدد. يمنع استخدام الحساب الشخصي للاستخدام المستنزف للمصادر. يحتفظ مركز تقنية المعلومات بالحق في إلغاء أي اتصال يتبين له أنه مستنزف للخدمة أو أنه في وضع غير مفعّل لمدة طويلة.
24. يمكن فقط الوصول الى الإنترنت باستخدام شبكة الإنترنت الخاصه بالمدرسة. لا يجوز استخدام أي طريقة أخرى للوصول الى النترنت داخل المدرسة. توصيل إنترنت تجاري و ربطه بشبكة المدرسة من دون علم مركز تقنية المعلومات و أخذ موافقة خطية بذلك. ممنوع منعاً باتاً.
25. يمنع تحميل جميع أنواع البرامج من الإنترنت وتثبيتها على أجهزة الحاسب الآلي الخاصة بالمدرسة. وفي حال ضرورة تنزيل برامج تخص العمل يرجى التواصل مع وحدة الدعم الفني في مركز تقنية المعلومات.
26. لمزيد من الحماية الوقائية من الفيروسات يمنع استخدام الفلاشات والأقراص الضوئية من أجل سلامة الشبكة و الحفاظ على خصوصية المعلومات وفي حال الضرورة لا بد من أخذ تصريح من مركز تقنية المعلومات
27. يكون استخدام أجهزة الكمبيوتر والنهيات الطرفية المتصلة بالسيرفر ضمن وقت الدوام الرسمي. (وفي حالة خارج الدوام الرسمي لا بد من رفع أسماء الموظفين إلى مركز تقنية المعلومات).
28. يمنع تزوير هويتك على شبكة الإنترنت كشخص آخر. (انتحال شخصية في شبكة الإنترنت).
29. يمنع استخدام الإنترنت بشكل يعرقل استخدام الآخرين مثل نشر الفيروسات .
30. يمنع دخول مواقع مشبوهة للإختراق و تنزيل برامج اختراق أو تجسس على أجهزة المدرسة أو الأجهزة الشخصية داخل المدرسة.

31. يمنع اختراق مواقع أو أجهزة داخل أو خارج شبكة المدرسة بأستخدام أي أجهزة أو أي طريقه كانت بقصد أو من دون قصد.

32. يحق للمدرسة اتخاذ الإجراءات التي تراها مناسبة في حق من يخالف هذه الضوابط

33. تحتفظ المدرسة بالتعديل في هذه السياسة عندما يستلزم الأمر ذلك.

عند التوقيع على هذه السياسة تعتبر ملزمة.

موافق ( ) الأسم: \_\_\_\_\_ المهنة: \_\_\_\_\_

غير موافق ( ) التوقيع: \_\_\_\_\_