West Kirby Grammar School

Digital Safety Policy

Approved by:	Governors' Quality of Education Committee
Last reviewed on:	November 2023
Next review due by:	Autumn 2025

Introduction

West Kirby Grammar School provides staff, students, parents and associates with access to a wide range of resources via a carefully monitored and maintained network. This type of environment requires users to demonstrate a responsible approach to the use of these resources and necessitates regulations to govern how equipment is used and what type of information is accessed.

The aim of this policy is to outline what is acceptable use of the School's IT equipment, network and the Internet and email. It is the intention of the policy to protect network users as well as the School against malicious and unintentional threats to the IT systems.

This policy applies to all users of the IT equipment at West Kirby Grammar School including: students, staff, governors, associate teachers, parents/carers and visitors to the School. It also includes accessing the School network from outside of the School premises via platforms such as Home Access Portal, Google Classroom and Remote Desktop Connection.

The policy is divided into the following sections:

1. General use of the School Network

Authorised users are given a unique username and password generated by the Network Manager. Individual users are responsible for their own password security **(See Appendix 1 – Password Security Policy).**

All users should be aware that their use of the School network will be monitored. The School reserves the right to examine or delete any files that may be held on its network.

The transmission, storage or collection of offensive, obscene or harassing material is strictly forbidden. If there is any doubt as to whether particular materials are acceptable then students should query this with the IT Services team who will make a decision on it.

Security of the School IT systems is maintained by the following methods:

- Appropriate security strategies as advised by the LA are implemented where appropriate for the School.
- Virus protection and firewall systems will be implemented and updated regularly.
- Software updates will be applied regularly.
- Hardware brought into the School will not be permitted on the School systems without specific authorisation and virus checking.
- User activity will be monitored using 'Impero' monitoring software.
- Adequate consideration should be given to the physical security of rooms containing sensitive information and IT equipment. As far as practical only authorised persons should be allowed access to rooms that contain servers or provide access to data.
- Users of the network should ensure that they use a password which follows the guidelines in the **Password Protection Policy (See Appendix 1)**

2. Use of Hardware

- If you are aware of a fault/malfunction when using IT equipment you should report it immediately to the IT Services team.

- No member of staff should install hardware components onto School equipment, without prior consultation with the IT Services team.

- Fixed IT computing equipment should not be moved to another location without prior consultation with the IT Services team.

3. Use of Software

- Only software which is legally owned by the School may be installed on computer equipment owned by the School. This includes games, screen savers and any other executable program.

- Only IT Services team staff should install software on computer equipment and/or the network.

- The unlawful copying of any copyrighted software and/or its use on School equipment is prohibited.

- Deliberate deletion or modification of software without prior approval from the IT Services team is prohibited.

- Deliberate introduction of a virus or any other malicious software to a computer/School network is prohibited.

- No user shall modify a computer's software, settings or other stored information; or attempt to access, copy, modify or disseminate information that is not intended for their use or bypass any security systems that are in place for the users' safety.

4. Use of Personal Devices (BYOD)

- Users may wish to connect their personal laptops to the School network. Users are granted access to School IT resources, both workstations and the connected network, only in terms of this policy and the condition that they observe these regulations.

- There is no expectation of privacy on computers connected to the School systems. Both technical and teaching staff may examine a student's laptop for educational, technical or disciplinary reasons at any time.

- Before a laptop is connected to the network, the user must ensure that it has appropriate virus checker, firewall software and an automatically updating version of the operating system to avoid the risk of damage to the School network. If unsure of how to complete this process – seek guidance from the IT Services team.

- The School takes all reasonable steps to protect the network from harmful software and other threats, however the School cannot accept responsibility for any damage which occurs to a student's computer or software as a result of connecting to the network or of transferring any data or information from the network.

5. Internet and Email Use

a. The Internet in the Curriculum

Internet access will be planned to enrich and extend learning activities. Pupils will be given clear objectives for Internet use. Pupils will be guided to take responsibility for Internet access by selecting appropriate sites and rejecting sites containing inappropriate material.

Pupils will be taught to:

- Validate information before accepting it is accurate.
- Compare the Internet with other media.
- Determine when an Internet resource is more appropriate than other resources such as books, papers, personal research.
- To acknowledge sources of information by indicating the internet locations used
- Be aware that it is not always possible to identify the person sending an e-mail or creating a web page accurately.
- Inform a teacher when faced with material they feel is inappropriate or offensive.

IT Support staff will ensure that:

- Filtering software (SonicWall) and monitoring software (Impero) will be active and applied to all computing devices connected to the school network.
- SonicWall and Impero will be updated as required.
- Lists of content/key words deemed “inappropriate” will updated regularly.

Teaching staff will ensure that:

- Student use of computing devices in their classroom is monitored using Impero.
- Should they discover any inappropriate content being accessed by students, this is reported to IT support to add this to the list of blocked content (as well as being reported via MyConcern)

No system for filtering and monitoring can be completely effective. Final responsibility for material accessed resides with the user.

b. General Internet Use

As far as possible, the School’s Internet Service Provider restricts access to websites which have been reviewed and evaluated prior to use but this cannot be guaranteed.

All users are expected to behave in a legal, moral and ethical fashion that supports the School’s aims and objectives.

The viewing, downloading, copying or transmission of any offensive, pornographic or extremist material on any item of equipment owned by the School is strictly prohibited and where applicable, the local authority and/or police may be informed should this occur.

Internet access is made available to students on the understanding that it may only be used for purposes related to the student's programme of study and not for profit, entertainment or other unrelated purposes.

Plagiarism is unacceptable. Any material accessed on the computers should be used in an appropriate manner in assignments and its source suitably noted.

c. E-Mail Use

E-mail in the School is regarded as public and can be monitored. There is no expectation of privacy.

Pupils will be taught that they have responsibility for any e-mails sent from their address and should therefore keep all passwords and usernames secure and confidential.

Staff are reminded that for their own protection they should only use the School provided email systems for communication with pupils and parents so that an audit trail can be maintained. Use of other systems may leave members of staff open to allegations of misconduct. This also applies to the use of other systems such as Skype.

Users are responsible for all e-mails sent. For staff, the same professional levels of language and content appropriate to letters and other media should be applied.

The School e-mail system is not to be used for any other purpose other than school business. It should not be used for any personal correspondence, contact with companies/organisations not associated with the school, or used to sign up for social media or other online accounts.

Staff are not expected to reply to emails outside of normal school working days and times.
They may choose to do so, but this is not to be expected.

Emails received by staff will be responded to within 2 working days. Emails sent in the evening will be considered to have been received the following morning and emails received over the weekend will be considered to have been received on Monday, or the next working day if this is not applicable.

For emails sent internally between staff: individuals named in the 'To' section are expected to respond by the sender, whereas those who have been CC'd are not and the message is for their information only. This helps to prevent multiple members of staff responding to the same message when this is not needed. This does not apply to emails sent to groups of users (e.g. 'Staff' or 'Teachers') where the contents of the message will determine whether a response is required.

6. Confidentiality of Data

All data accessed through systems such as ARBOR and SISRA should be treated as confidential and not copied/shared with any parties.

Users should also take every precaution to protect the sensitive data that they interact with. Users should not store sensitive information on personal devices and should report the potential loss of any sensitive data immediately.

Providing non-Public information to external parties should not occur without prior approval of the Head Teacher.

Users of systems which contain confidential data (ARBOR/SISRA for example) should make sure that this information is not displayed to pupils or other parties the data is not intended for. Users should make sure that such data is never projected on an interactive whiteboard and that computers are locked when not attended.

Confidential data should not be copied to storage devices and taken out of the school without adequate measures to ensure the security of the data such as using an encrypted storage device.

7. Staff Social Media Use

Staff should be aware that information that they publish on any site on the Internet, including social networking sites, could possibly be seen by pupils, parents and other stakeholders in the School. Care should be taken to set privacy settings on sites appropriately and to avoid publishing material that could cause embarrassment to the member of staff concerned or to the School (this could include comments or images about the School, pupils or personal activities).

Pupils, parents and other stakeholders should not be added as ‘friends’ to social networking sites. This also applies also to pupils who have recently left the school. A suitable alternative approach may be to have two entries on the site, one for School contacts and the other for personal/private use which is not available to School contacts.

It should be noted that the publishing of inappropriate material could result in disciplinary action against the member of staff concerned. If a member of staff is uncertain whether particular material is appropriate they should seek guidance from the Headteacher.

8. Web Publishing – School Website and Social Media Accounts

The School website and social media accounts have been designed to provide information about the School and to provide opportunities to disseminate information to parents as well as to promote the school in the wider community. All public communication to parents and routine notices will be made available on the website.

As the website and social media pages can be accessed by any computer outside the School the security of staff and pupils is paramount. The publishing of names beside photographs that identify individuals is acceptable with parental permission, but remember some students should not be identified at all. Personal information or contact details must not be published without written consent.

The Headteacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained; All material published must meet copyright legislation.

The point of contact on the web site and social media accounts will be the School address and telephone number. Personal information and e-mail addresses will not be published.

All posts on school social media accounts should be appropriate, use a professional tone of language and reflect the aims and values of the school. They should be student centred and department lead, ensuring that all published posts that are for the benefit of the students.

If a member of staff is uncertain whether particular material is appropriate for publication on social media accounts, they should seek guidance from the School Social Media Coordinator or a member of the Senior Leadership Team.

9. Remote Learning

We will aim to ensure the ongoing education of our pupils under unusual circumstances such as school closure from illness epidemic, extreme weather, power-loss, etc. through the provision of remote learning.

Such remote learning may also be appropriate in situations when students, in agreement with the school, have a period of absence but are able to work from home.

Please see **Remote Learning Policy** document.

10. Cyberbullying

The School's definition of cyberbullying is **'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'**

In order to reduce the potential for cyberbullying children must have their phones switched off, in their bags when in School and put 'out of sight, out of mind'.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Staff are encouraged to report all incidents of cyberbullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

11. Failure to comply with Acceptable Use Policy

Users who fail to conform to this acceptable use policy may be required to pay for repairs to and replacement of any damaged equipment and the resources and time used by IT staff in investigating and correcting the situation. Students may have their access to IT facilities withdrawn by the IT staff. Serious cases or repeated offences may be reported to the Headteacher and may result in disciplinary action. The School will cooperate with any external agency who believes a West Kirby Grammar School user is engaging in any illegal activities.

If you have any questions regarding this policy or the Internet, Email and IT Security Policy, please speak to the Head Teacher or a member of the Senior Leadership Team.

Acceptance of the Policy

I have read and understand the Acceptable Use Policy, including the consequences of violations listed above, and agree to abide by these policies.

Name (please print)		**Signature**		**Date**		

Appendix 1 - Password Security Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of WKGS resources. All users, including contractors and vendors with access to WKGS systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at West Kirby Grammar, has access to the West Kirby Grammar network, or stores any non-public WKGS information.

Policy

1. Passwords for all systems should consist of 8 or more characters, consisting capital letters, lower case and numbers.
2. Where possible, users must use unique or a varied password between systems unless the system in question has synchronised single sign on.
3. User accounts that have high system-level privileges must have a unique password from all other accounts.
4. Users will be expected to use multi factor authentication where applicable.
5. Passwords must not be revealed over the phone to anyone.
6. Do not write down passwords and store them anywhere that isn't secure.
7. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
8. Passwords must not be shared with anyone. All passwords are to be treated as sensitive.
9. Passwords must not be inserted into email messages
10. Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on holiday, and family members.
11. Do not leave any pc, laptop or device unlocked while unattended. Any unattended device must be locked.