Wellington Area Rural Federation

Stawley Primary School

IT Acceptable and Fair Use POLICY

September 2024

Status:	STATUTORY
Responsible person:	HEADTEACHER
Responsible Governor :	CHAIR OF GOVERNORS
Ratified by the Head Teacher:	September 2024
Date first approved by the Governing Body:	September 2020
Review Period:	Annually
Review Date:	September 2025

This policy document contains two sections. The first explains the core regulations of the policy, The second contains guidance notes explaining the regulations in more detail and giving guidance of best practices to ensure users understand how they can best comply with the regulations

Purpose

This policy is intended to promote ICT best practices among the School's employees, partners and other ICT users. This policy should be read in conjunction with the School's existing policies and procedures. Protecting the School's School ICT facilities is a team effort involving the participation and support of every user of our School ICT facilities. It is the responsibility of every ICT user to know and comply with this policy.

The purpose of this Acceptable Use policy is to enable the School to:

Outline the acceptable use of its School ICT facilities, and

Set regulations to protect the School and its employees, pupils and other ICT users.

Inappropriate use exposes the School to risks including malicious attacks, compromise of network systems and services, and legal issues. In general, acceptable use covers everything including respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent license and contractual agreements.

Summary principles

Governance
Don't break the law
Abide by The School's Code of Conduct and all other Policies, Standards and Guidance
Abide by third party regulations for any facilities you access

Infrastructure
Don't interfere with hardware
Don't take risks by performing actions that may introduce malware (see 2.7) onto the School network or School
Don't load unauthorised software

Behaviour
Take care of all equipment issued to you and take steps to avoid accidental damage, loss or theft
Don't waste ICT resources

Identity
Don't allow anyone else to use your ICT credentials for any system or service (login ID and password, smart to
Don't use the ICT credentials of anyone else
Don't disguise your identity or deliberately bypass any security controls

Information
Always consider data security when storing, processing or transmitting information.

Contents

1. Core regulations

1.1 Scope

This policy applies to anyone using the School's ICT facilities including staff, partners, suppliers and anyone accessing externally published services such as the School website.
School ICT facilities includes all hardware, software, data and voice systems, internally and externally published services and third party systems and services. It covers all School ICT resources, services, facilities, systems or devices whether connected directly, indirectly or remotely to the network irrespective of location or the location of the user.

1.2 Governance

The School abides by all laws in England and Wales.

1.3 Authority

This policy is issued by the School's governing body which is responsible for its interpretation and enforcement, and which may also delegate such authority to other people, such as the Headteacher.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority to enforce this policy. If you feel that any such instructions are unreasonable or are not in support of this policy you may appeal to the School's Data Protection Officer.

The School reserves the right to introduce supporting policies, standards, processes and guidance to support, enforce and clarify specific elements of this policy where appropriate. In such cases these will be subject to review and approval from the governing body and/or Data Protection Officer.

1.4 Intended Use

The School ICT facilities are provided to support delivery and fulfilment of the School's vision and priorities in delivering education and safeguarding the welfare of the pupils and staff members of the School.

1.5 Personal Use
Staff may use School ICT facilities for personal use if it does not breach anything in this policy. Personal use is subject to the same management policies as any other non-work activity. Personal use of School ICT facilities must only be done outside of working hours – i.e. during lunch breaks or before/after work.

It is not permitted to store your personal data on any School ICT facilities that is not work-related, including but not limited to email, network shares, Microsoft SharePoint or Microsoft OneDrive or any element of the School Office 365 environment without prior authorisation from the School. The School accept no responsibility for any loss/damage or authorised/unauthorised access of this type of data. You should be aware that there are circumstances where personal information stored on or transmitted through School ICT facilities may be viewed by authorised personnel in accordance with the School's Data Protection Policy.

You are not permitted to connect any personal device to any part of the School ICT facilities without the express permission of a senior member of staff. This includes connecting personal mobile phones, even for charging, to school laptops, or connecting personal laptops to the network without authorisation from the appropriate person at the School.

The only exception to this is that you may connect personal devices up to networks that are specifically provided for this purpose such as the Guest networks.

School staff must not use personal social media with any child with whom they solely have, or have had, a staff/pupil relationship. This includes ex-pupils until they reach the age of 18.

Staff can have social media contact with pupils or ex-pupils where other appropriate relationship exists, for example a family member or family friend. These relationships must be open and transparent and the member of staff can report these to senior leaders for their own protection.

Personal opinions must not compromise the professional role of staff members, nor bring the school into disrepute. Staff must take all reasonable steps to ensure the proper separation of their personal and profession lives.

1.6 Commercial Use
You may not use any School ICT facilities for commercial purposes or for financial gain at any time.

1.7 Identity (including passwords)
You must take all reasonable precautions to safeguard any ICT credentials (usernames and passwords, email addresses) issued to you. This includes ensuring your password is secure; the School encourages the use of strong passwords including those that are at least six characters and a combination of upper- and lower-case letters, numbers and symbols.

You must not allow anyone else to either see or use your ICT credentials. This forbids logging in with your ID on behalf of a colleague or pupil. You must not attempt to obtain or use anyone else's credentials. Issues with logging in should be reported to the appropriate person. If somebody does ask for your password it should be reported immediately to the appropriate person.

You must not attempt to obtain or use anyone else's credentials unless you are an appropriate person with permissions. This forbids logging in on behalf of colleague or pupil. Issues with logging in should be reported to the School.

You must be mindful of what data is on the projector during lessons and ensure that personal details are not displayed publicly i.e. registers.

If you have reason to believe that somebody else may know your password, you must change it immediately.

If you have reason to believe that somebody else has logged in using your credentials then this must be reported to the Senior Leadership Team immediately who will then decide on further action.

You must not allow unauthorised persons access to any end user devices (including laptops, mobile phones, tablets) that are connected and authenticated to any School system or service.

You must not respond to any unexpected or unsolicited communications requesting your details/login credentials or follow any links from such communications.

You must not impersonate, or attempt to impersonate someone else or disguise your identity when using School ICT facilities. This includes you not using a colleague's account, even if they have either given you permission to, or an instruction to do so.

Screens should be set to auto lock after a maximum of 3 minutes without usage and the school's local ICT technician will implement this.

1.8 ICT Infrastructure

ICT Infrastructure is a term which covers all School ICT service components (e.g. hardware, software, data, internal and external ICT services, contracted ICT services) which are employed by the School. You must not do anything to jeopardise the integrity of the ICT infrastructure by, for example, doing any of the following:

X Damaging ICT equipment
X Transferring equipment away from the registered owner
X Failing to report any lost or stolen equipment to the School
X Reconfiguring School ICT equipment or Systems without approval
X Moving equipment without approval
X Installing or loading software on School ICT equipment other than in approved circumstances
X Attaching unauthorised devices to School ICT equipment
X Reconfiguring or connecting equipment to the network other than by approved persons and methods
X Setting up unauthorised servers on the network
X Deliberately, negligently or recklessly introducing malware
X Attempting to disrupt or circumvent any ICT security measures
X Releasing School controlled data/information onto unauthorised ICT infrastructure including that of unauthorised third party suppliers

1.9 Equipment care

School laptops or computers must be shut down when not in use for long periods of time to conserve electricity.
Reasonable care must be taken to protect any physical equipment (laptops, mobile phones/devices, printers) that users have access to, both from a device and data security point of view.

You must urgently report any lost or stolen hardware (laptops, mobile phones) to ICT and the Senior Leadership Team to limit the risk of data loss. ICT may disable accounts or remotely wipe devices where possible, to assist with data protection.

1.10 Information
Staff that handle personal, confidential or sensitive information must take all reasonable steps to safeguard it. You must be compliant with the Data Protection Act 2018 and GDPR and also must observe the School's Protection Policy and any relevant schedules, procedures and guidance around data protection.

You must take particular care with regard to the risks associated with the use of insecure wireless services, removable media, text (sms) messages, mobile and privately owned devices when processing or accessing such information.

You must not attempt to access, delete, modify nor disclose personal information belonging to other people without a lawful basis nor may you use personal information for any purpose other than that for which the data was obtained without the Data Subject's permission or the explicit written approval from the School's Data Protection Officer.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, violent, threatening or discriminatory.

You must not infringe copyright, or break the terms of licences for software or other material.

Staff must be aware that it is an offence to knowingly or recklessly obtain, disclose, retain or procure personal data without the consent of the School.

Upon leaving your employment, any personal data that does not belong to you, the employee, must be returned to the School. Any School agreed personal devices must be wiped clean of personal data that was necessary for processing under the authority of the School.

1.11 Remote Working
If you are working away from the School building (s) you must use password protected devices and approved methods of remotely accessing the School network or data. Further information about this can be found in section 2.11.

Avoid working in public areas when your keyboard and screen could be overlooked or places where your equipment is at high risk of theft.

Employees are reminded to lock their screens when they are not at their desk.

Personal data which falls under the control of the School must not be downloaded onto personal devices without authorisation from the Senior Leadership Team.

Whilst taking paper copies of work home, you must ensure that these are kept in a secure location (i.e. not left visible in cars or in the boot of a vehicle).

1.12 Working on personal devices
You are not to download personal data in relation to School data to your personal device without School permission, as this creates an unacceptable risk. Where School business is carried out on personal devices, this will not be carried out without School permission.

You must ensure that when using emails on personal devices, these are logged off when not in use to prevent the risk of unauthorised access.

1.13 International working

If you intend to take School ICT equipment (laptops, mobile phone/devices) outside of the United Kingdom for any period of time then you must seek approval and further guidance from Senior Leadership Team and the School's Data Protection Officer.

ICT equipment (laptops, mobile phones and other devices) may be blocked from working outside of the United Kingdom unless the Senior Leadership Team, ICT and the Data Protection Officer have been given time to assess and approve any international working requests.

1.14 Sanctions

If you are an employee the School's disciplinary processes will be used to handle breaches of this policy.

In addition, the Senior Leadership Team and School's governing body may impose sanctions including, but not limited to, restrictions on your ongoing access and use of School ICT facilities.

Illegal or suspected illegal activity will be reported to the relevant enforcement agency such as the police.

1.15 Contacts/References

School ICT/facilities Team Lead: Paula Maguire (Teacher)

2. Guidance notes

2.1 Scope

If this Policy is not adhered to, sanctions may apply, where relevant. For staff members, sanctions will be outlined in the School's disciplinary procedure. Visitors may have their access to School ICT facilities removed.

2.2 School ICT facilities

The term School ICT facilities includes but is not limited to:

Hardware provided by the School including laptops, mobile phones, tablets, USB sticks etc.;

Network infrastructure, including network cables and sockets, network switches, wireless infrastructure;

Software provided by the School including operating systems, office applications, web browsers, line of business applications etc.;

Data that the School processes, stores and transmits or provides access to.

Access to the internet;

Approved online services hosted elsewhere such as (but not limited to) Office365, SharePoint and Capita software;

ICT credentials, such as your network login, email address or smart token.

2.3 Absence

Access to absent staff ICT accounts, by staff other than the account holder, may be granted in circumstances where members of staff have an unplanned absence, or are on sick leave, or on holiday or have been suspended from work or left the School. Under these, or similar, circumstances your line manager may request access to your account including access to emails and files stored on your network shares to facilitate the normal running of School business or in the process of complying with a Subject Access Request. Requests for this type of access must be logged with the Data Protection Officer and will be processed by the appropriate person with the ability to facilitate this, under the authorisation of the Senior Leadership Team. Requests for access due to planned leave will not be granted.

You can reduce the risk of this happening by storing documents and data relevant to other staff in team or shared areas of the network.

2.4 Equipment care

You should take care of any School issued equipment as if it was your personal equipment with due respect for the hardware and for protection of the data stored upon it.

One of the most common reasons for a School device being stolen is that it has been left overnight in a car. Leaving a device in plain sight in a car or in a car overnight is not acceptable. It is also unacceptable to leave School issued equipment unattended in public areas.

Take care when handling or using equipment to ensure that it isn't damaged through accident, dropping or improper use.
Laptops must also be shut-down or restarted every day to ensure that they receive security patches and software updates. If a device isn't likely to be used for a long period of time or the current user has left then it must be returned to the School.

2.5 Identity
You must take all reasonable precautions to safeguard any ICT credentials issued to you:
You must ensure your password is secure.
This means that you must change passwords when first issued and at regular intervals or as instructed.

X Do not use obvious passwords, and do not record them where there is any likelihood of someone else finding or accessing them.
X Do not share passwords with anyone else, not even with your manager, family or any member of staff, no matter how convenient and harmless it may seem.
X Usernames and passwords or PINs must never be attached to devices or stored in notepads in laptop bags. This behaviour is unacceptable and creates a serious risk of a breach of both data stored on the device and data accessible by remote access methods. These incidents are reported to the Data Protection Officer and in certain circumstances to the Information Commissioners Office (ICO) which could result in a significant fine for the School.
X Do not use your School username and password to log in to web sites or services you do not recognise, and do not log in to web sites that are not showing the padlock symbol. Dependant on the Internet browser you are using the padlock symbol will appear in different places but always around the website address bar normally towards the top of the browser page:

X Do not store your credentials in untrusted devices, including auto-complete or auto-login in web browsers.
X Do not click on links contained in unexpected, unsolicited emails.
X Do not leave logged in computers unattended in an unlocked state.
X If you have not been able to comply with this guidance or the policy content for whatever reason, please report the matter to the SLT.

2.6 Email
Care must be taken when addressing emails, particularly those including sensitive or confidential information, to avoid accidentally sending them to the wrong people. Particular care must be taken when the School email provider auto-completes an email address and when a 'reply-to-all' option is used.

Emails should not be auto-forwarded to any other account as this may result in sensitive or confidential information being disclosed to unauthorised people.

2.7 Malware
Malware is a generic term to describe software or code that provides any unwanted computer operations. Common variants are viruses, worms, trojans and ransomware.

You must take all reasonable precautions to avoid introducing malware to the network or onto devices. The main risks to be avoided are:

X Opening suspicious external emails that either contain attachments or web links
X Browsing to suspect websites and/or trying to download software
X Connecting untrusted/personal devices such as USB sticks or mobile phones

2.8 Sanctions

If you are an employee the School's disciplinary processes will be used to handle breaches of this policy.
Illegal or suspected illegal activity will be reported to the relevant enforcement agency such as the Police.

2.9 Personal Use
No personally subscribed to service belonging to staff, including but not limited to, personal email accounts (e.g. Yahoo, Hotmail, Gmail etc.), personal social media accounts (e.g. Facebook, Twitter), or personal storage accounts (e.g. Dropbox, Google, Personal OneDrive, iCloud etc.) may be used for work purposes. No School controlled personal data may be sent to or stored in any such personal accounts.

2.10 Behaviour
You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening or discriminatory.

2.11 Remote Working
If you access personal data remotely, you must make sure you are using an approved connection method capable of ensuring that the information cannot be intercepted between the device you are using and the source of the secure service. The most common approved connection methods for remote working would be:
You must also be careful to avoid working in public locations where your screen can be seen.
Where devices are stored in the home of the user, they must not be left on display, by windows for example, unless in use. See also 1.11.

2.12 Removable media
Personal data in relation to the School must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet or smart phones) unless it is owned by the School and encrypted with the key kept securely.

2.13 Excessive Consumption of Bandwidth / Resources
Use resources wisely. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do or in colour when monochrome will do. Do not waste electricity by leaving equipment needlessly switched on. The School's ICT and the Senior Leadership Team reserve the right to charge employees for any costs incurred due to the excessive consumption of bandwidth / resources.

2.14 Monitoring
You must not attempt to monitor the use of School ICT facilities without the explicit permission of the Senior Leadership Team. This would include:

- **X** Monitoring or interception of network traffic
- **X** Network and/or device discovery
- **X** Wi-Fi traffic capture
- **X** Installation of key-logging or screen-grabbing software that may affect users other than yourself
- **X** Attempting to access system logs or servers or network equipment

2.15 Compliance (Investigation, Monitoring and Reporting)
The School monitors and records the use of its School ICT facilities for the purposes of business continuity, capacity planning, the detection and prevention of infringement of this and other School policies and the investigation of alleged misconduct or breach of the law.

In order to protect the School's ICT assets, services and reputation, under the authorisation of the Governing Body and/or the Senior Leadership Team, the School reserves the right, when reasonably necessary, to access and monitor the content of School systems or services. Additionally, monitoring is carried out in order to further protect the integrity of those systems/services, the rights of other users and the observance of the law.

Monitoring may include, but is not limited to, access to user accounts; access to network files and folders; examination of logs; details of website accessed; emails; mailboxes; telephone records including instant messaging; sign-in access; and other checks on user compliance in-line with current policies, paying particular attention to the School's Data Protection Policy.

Users should bear these factors in mind when deciding whether to use School provided facilities for personal use.
The School also reserves the right to undertake, without prior notification, monitoring of the use that any individual user/s is/are making of those systems/services. Where such monitoring or records examination is invoked, it is always subject to a high level of justification and authorisation and will be approved by the Senior Leadership Team and Governing body. The School will comply with lawful requests for information from government and law enforcement agencies.