Olga Primary School

Information Security Policy

Policy Date: May 2025
Review Date: May 2026

Introduction

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to:

- Protect against potential breaches of confidentiality.
- Ensure that all information assets and IT facilities are protected against damage, loss or misuse.
- Support our Data Protection Policy in ensuring all Staff are aware of and comply with UK law and our own procedures applying to the processing of data.
- Increase awareness and understanding at the School of the requirements of information security and the responsibility to Staff to protect the confidentiality and integrity of the information that they themselves handle.

Information Security can be defined as the protection of information, including any biometric data and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy. Online Safety Policy and Acceptable Use Policy for further information. These Policies are also designed to protect personal data and can be found on the shared area.

For the avoidance of doubt, the term 'mobile devices' used in this Policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones & watches.

Scope

The information covered by this Policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, cloud storage, paper records, hand-held devices, and information transmitted orally.

This Policy applies to all members of Staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of Staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this Policy will be treated as a disciplinary offence which may

result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This Policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this Policy in order to remain compliant with legal obligations.

This Policy will apply to the following data systems:

1. SIMS Connected - Hosted MIS Data.
2. SIMS Teacher App – Access to SIMS Data.
3. Schoolcomms and School Gateway - Communications and Sales.
4. SIMS Parent App – Online Activity Booking System for Parents/Carers, including access to pupil records to update personal information held on the local server.
5. SIMS Applicaa – Online Admissions System for new intake in Nursery and Reception.
6. SIMS School Cloud – Online Parents Meeting App.
7. LGFL – Pupil and Staff data for emails and user accounts.
8. LGFL VOIP – Staff Data for phone system and call recording.
9. LGfL Gridstore - Remote Data back-up.
10. NET2 – Access Control System – Staff Names.
11. Inventry – Sign in system for all Staff/Visitors/Parents/Carers/Contractors/Pupils.
12. SAGE 200 Cloud – Finance System for billing/crediting Parents/Carers and Staff where necessary, holding names and Bank Account details.
13. SAGE 50 Payroll Cloud – Staff Payroll Data.
14. Lessons Learned – Staff Performance Management Data.
15. Otrack – Pupil Performance Data.
16. CPOMS – Child Protection and Behaviour Logging.
17. CCTV – 35 Day continuous recording, all external areas of the School and some internal areas.
18. Iron Mountain – Off-site Data Archive (Pupil/Staff records, Financial Information).
19. Apple School Server & Meraki – Staff/Pupil Data.
20. Parago / Civica – Asset Management.
21. Google G Suite – Staff/Pupil Data.
22. School Bus – Online Policy Compliance Suite – Staff Data.
23. Papercut – Staff data for print management.
24. Foldr – Remote Data Access System – Staff Data.
25. Corlytics [Clausematch] - Policy Management Portal.
26. SAM People - Cloud based Staff Absence Management System.
27. Tapestry - EYFS software to record observations with parental access levels.
28. Medical Tracker - A cloud based system to record all First Aid and Medical issues.
29. TES - Online Jobs Portal.
30. The Key - Online support and guidance on Leadership/Management
31. 3rd Party Curriculum Software - including White Rose, Twinkl, Testbase & Apple apps.

1. General Principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the SBM the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of Staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the SBM or by such third party/parties as the SBM may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the SBM unless expressly stated otherwise.

All Staff have an obligation to report actual and potential data protection compliance failures to the SBM who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

2. Cloud Based / Off-Site Data Storage

All the data systems listed above involve cloud and/or off-site storage, except CCTV and building access.

When choosing such systems, the School has a written undertaken about the security of the data and that data transfer is encrypted. The systems also have appropriate levels of hierarchy to ensure data protection.

3. Physical Security & Procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Lockable cupboards shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on Staffroom tables, or pinned to noticeboards where there is general access

unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of School.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the SBM as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The School undertakes regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School has a controlled entry system to minimise the risk of unauthorised people entering the School premises.

CCTV Cameras are in use at the School and monitored by as described in the CCTV Policy.

Visitors should be required to sign in at the reception, accompanied at all times by a member of Staff and never be left alone in areas where they could have access to confidential information.

4. Computers & IT

The SBM/Designated Lead of Computing, shall be responsible for the following:

a. Ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements.
b. Ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management.
c. Ensuring that all members of Staff are kept aware of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, the SBM shall be responsible for the following:

a. Assisting all members of Staff in understanding and complying with this Policy.
b. Providing all members of Staff with appropriate support and training in IT Security matters and use of IT Systems.
c. Ensuring that all members of Staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements.
d. Receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer].
e. Taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of Staff.
f. Monitoring all IT security within the School and taking all necessary action to implement this Policy and any changes made to this Policy in the future.

g. Ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

5. Responsibilities – Members Of Staff

All members of Staff must comply with all relevant parts of this Policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the SBM of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the helpdesk of Connetix immediately.

You are not entitled to install any software of your own without the approval of the IT Technician. Any software belonging to you must be approved by the IT Technician and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

If you detect any virus this must be reported immediately to the IT Technician (this rule shall apply even where the anti-virus software automatically fixes the problem).

6. Access Security

All members of Staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this Policy.

The School has a secure firewall and anti-virus software in place, supplied by LGfL. These prevent individuals from unauthorised access and to protect the School's network. The School also teaches individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular cloud based) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods, such as fingerprint recognition are encouraged where the technology is available.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the SBM/Headteacher as appropriate and necessary. Any member of Staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of Staff who logs on to a computer using another member of Staff's password will be liable to disciplinary.

If you forget your password, you should notify the IT Technician to have your access to the IT Systems restored.

You should not write down passwords if it is possible to remember them.

Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this time period or disable the lock.

All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this Policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

7. Data Security

Personal data sent from the School will be encrypted or otherwise secured. This is possible by either encrypting files using Adobe, Word or Excel settings or using 3rd party software like Egress.

This password should be communicated to the recipient via a phone call or by another secure means, but NOT using the same method as for transferring the file.

All members of Staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from IT Technician who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this Policy). The SBM may at any time request the immediate disconnection of any such devices without notice.

8. Electronic Storage Of Data

All data, and in particular personal data, should only be stored on Foldr, which is secure and encrypted. If you want to use a USB, it should be encrypted.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

9. Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the SBM. All members of Staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the SBM shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of Staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the SBM. Any attempt to resolve an IT security breach by a member of Staff must be under the instruction of, and with the express permission of, the SBM.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the SBM.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

10. Related Policies

Staff should refer to the following Policies that are related to this Information Security Policy:

- Online Safety Policy / Acceptable Use Policy
- Data Breach Policy
- Data Protection Policy (GDPR Compliant)