WAULUD PRIMARY SCHOOL

GDPR - INFORMATION SECURITY POLICY

Document Status - Statutory	
Author	SPT Compliance - Business Manager
Date of Origin	April 2020
Revised	November 2025 - Revision April 2026
Version	1
Review Requirements	Annually
Date of Next Review	Spring 2028
Approval Body	Resources Committee
Publication	School Website/Staff Share

Agreed by Governors:
November 2025

Table of Contents

1 Introduction.....3

2 Scope.....3

3 General Principles.....3

4 Physical Security and Procedures 3

5 IT Security and Procedures 4

6 Access Security.....4

7 Data Security.....5

8 Home Working 5

9 Communications, transfer, internet and email use 5

10 Reporting security breaches 6

WAULUD PRIMARY SCHOOL

"Working together to provide a safe, inclusive learning environment where all are valued, respected and achieve their very best.
Challenges are met with determination and welcomed as opportunities to flourish and grow."

1. Introduction

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 require organisations to protect the rights of individuals whose personal data is stored and processed, and to take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

School is dedicated to ensuring the security of all information it holds and aims to implement appropriate and effective standards of information security 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 of staff to protect the confidentiality and integrity of the information that they themselves handle.

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.

2. Scope

The information covered by this policy includes all written, and electronic information held, used or transmitted by or on behalf of the school. This includes information held on computer systems, paper records, hand-held devices, including information transmitted verbally where it is recorded or forms part of a structured filing system.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and all third parties authorised to use the IT systems. All the above 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, or appropriate action according to the relevant procedures for the post holder.

3. General principles

Staff should discuss the appropriate security arrangements for the type of information they access in the course of their work with the data protection lead in school. All data stored on our IT Systems and our paper records shall be available only to members of staff with a 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 school data protection lead. 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 school data protection lead unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the school data protection lead 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 by the school's GDPR lead.

Access to information should be limited to those who require it for their role (need-to-know basis), and permissions should be regularly reviewed.

4. Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information should 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. This includes when working from home.

Available locked filing cabinets and locked 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 or in publicly accessible areas 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 must be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you consider the security to be insufficient, you must inform the school data protection lead as soon as possible. Increased risks of vandalism and or burglary shall be considered when assessing the level of security required.

- The school closes the school gates during certain hours to prevent unauthorised access to the building.
- An alarm system is set nightly.
- CCTV Cameras are in use at the school and monitored by the Headteacher/Business Manager
- 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.

5. IT security and procedures

All members of staff must always comply with all relevant parts of this policy 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 school data protection lead of all security concerns relating to the IT Systems which could or has led to a data breach as set out in

the Data Breach Policy, and any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems

You are not entitled to install any software on school devices without approval

Physical media (e.g. USB memory sticks) should not be used unless authorised and encrypted.

If you detect any virus this must be reported immediately (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. These prevent individuals from unauthorised access and to protect the school's network.

All passwords must, where the software, computer, or device allows:

1. a) be at least 8 characters long including both numbers, letters, and a special character (amend to meet your arrangement)
2. b) be changed on a regular basis;
3. c) not be obvious or easily guessed (e.g. birthdays or other memorable dates)
4. Passwords must be kept confidential and must not be made available to anyone else.
5. If you forget your password, you should notifythe school data protection lead to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

   You should not write down passwords. Computers and other electronical 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.

   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.

Multi-factor authentication should be used where available.

7. Data security

All members of staff are prohibited from downloading, installing, or running software from external sources without obtaining prior authorisation, bona fide requests for work purposes will be assessed. 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.

Personal devices must meet minimum security standards, including password protection and up-to-date security software (including, but not limited to; laptops, tablets, and smartphones) to the school's Wi-Fi provided that you follow the school's 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).

All school laptops will have encryption software in addition to individual user passwords.

8. Home working

You should not take confidential or other information home without prior permission of the Headteacher, and only do so where satisfied that appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that information is:

a) not transported in see-through or other un-secured bags or cases
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.)
c) not left unattended or in any place where it is at risk (e.g.in car boots, cafes, etc.)
d) kept in a secure and locked environment where it cannot be accessed by family members or visitors
e) all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

9. Communications, transfer, internet, and email use

When using the school's IT systems, you are subject to and must comply with the School's Acceptable User Policy. The school work to ensure the systems protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported immediately. Regular checks are made to ensure that filtering methods are appropriate, effective, and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee, and the school cannot accept liability for the material accessed or its consequence.

Personal information should be transmitted securely, using encryption where appropriate, before being sent by email or posted via recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, fax and email addresses and numbers should be checked and verified before you send information to them. You should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the school.

10. Reporting security breaches

All members of staff have an obligation to report actual or potential data protection compliance failures, or questions to the school data protection lead.

When receiving a question or notification of a breach, the issue will be immediately assessed, 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. Any attempt to resolve an IT security breach by a member of staff must be under instruction and with express permission.

Missing or stolen paper records or mobile devices, computers containing personal or confidential information should be reported immediately. All IT security breaches shall be fully documented.

All security breaches must be reported and managed in accordance with the school's Data Breach Policy.