RUSSET HOUSE SCHOOL

Information Security Policy

Author	?	Classification	OFFICIAL	Date of First Issue	May 2025
Owner	LBE	Issue Status	FINAL	Date of Latest Re-Issue	
Version	1.0	Page	TBC	Date approved by Governors	
Reviewer	DPO			Date of next review	2/2027

May 2026

CONTENTS

1 Policy statement 3
2 Introduction 3
3 Purpose 3
4 General principles 4
5 Risks 5
6 Roles and responsibilities 5
7 Data security 7
8 Access security 8
9 Physical security 9
10 Electronic storage of data 10

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

1 Policy statement

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

Russet House School (hereinafter referred to as 'the School') is dedicated to ensuring the protection of all information assets within the keeping of the School.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

The School will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information security policy within the school including the supporting guidance documents which are listed below.

This Policy 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 the School Data Protection Policy in ensuring all staff are aware of and comply with UK law and School procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility for staff to protect the confidentiality and integrity of the information that they process.

2 Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.

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

3 Purpose

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

Information is an invaluable asset to the School and must be protected.

The School relies on information to carry out statutory and other functions as well as to deliver services to residents.

Information assets of the School exist in many forms and this policy includes the protection of information stored electronically, transmitted across networks, and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud).
It includes the internet, but also the other information systems that support our businesses, infrastructure, and services.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the School maintains, it also addresses who has access to that information, the processes they follow, and the physical computer equipment used to access them.

The School is dependent on information being held safely and securely and implements appropriate technical security measures to enable them to provide assurances to pupils, parents, and staff, about the way that it looks after information. This ensures that individuals data privacy is protected, and their personal information is handled appropriately.
This policy details the basic requirements and responsibilities for the proper management of information assets, that are used by the school to operate securely.

4 General principles

All data stored on School IT systems is to be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information); to enable appropriate handling, in accordance with the level of sensitivity.

All data stored on School IT Systems or 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 nominated IT Consultant/s or by such third party/parties as authorised by the Headteacher.

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

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 Headteacher, unless expressly stated otherwise.

All staff have an obligation to report actual and potential security/ data protection compliance failures to the I.T security officer and the School Data Protection Officer (DPO) via the designated inbox. For data protection contact schools.data.protection.officer@enfield.gov.uk, who will advise on investigation and shall decipher whether there is a need to report to the ICO.

5 Risks

The School recognises that there are risks associated with users accessing and handling information, to conduct official school business.

The School is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the School to use all reasonable, practical, and cost effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure.
- The confidentiality of information will be assured.
- The integrity and quality of information will be maintained.
- Authorised staff, when required, will have access to relevant school systems and information.
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained.
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements.
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to staff on request.

Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and embarrassment.

6 Roles and responsibilities

It is the responsibility of each member of staff to adhere to this policy, standards, and procedures. It is the School's responsibility to ensure the

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

security of their information, ICT assets and data. All members of the School have a role to play in information security.

The Headteacher, in conjunction with the Senior Leadership Team and IT consultant 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 UK GDPR and the Computer Misuse Act 1990.

Furthermore, the IT Consultant, in conjunction with the Headteacher and Senior Leadership Team 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 relating 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; and

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.

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

All 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.

Staff must immediately inform the Data Protection Officer, (DPO) 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 a member of the Senior Leadership Team immediately.

Members of staff are not entitled to install any software of your own without the approval of the Headteacher. Any software belonging to you must be approved by the Headteacher 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. Prior to installation of any software onto the IT Systems, you must obtain written permission by the Headteacher. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files. The Headteachers approval must be obtained prior to transferring of files using cloud storage systems.

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

7 Data security

Personal data sent over the school network will be encrypted or otherwise secured.

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Headteacher 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 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). The Headteacher may at any time request the immediate disconnection of any such devices without notice.

8 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. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.
All IT Systems (in particular mobile devices) 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 can only be used if approved by the IT Department. All passwords must, where the software, computer, or device allows:
a) be at least 6 characters long including numbers, letters, and a special character (e.g. $%£); b) be changed on a regular basis;
c) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the IT Consultant 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

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password, you should notify the IT Consultant and a member of the Senior Leadership Team 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 and should aim to remember them. You may wish to write down a memorable word that you store securely (e.g. in a locked drawer or in a secure password database), to assist with remembering the password.

The memorable word/phrase (and passwords) should never be left on display for others to see. 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 short period of inactivity. You may not change this 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.

9 Physical security

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.

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 where there is general access unless there is legal reason to do

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

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 find the security to be insufficient, you must inform the Headteacher 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 carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The School close 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 Office Staff. Visitors are required to sign in at 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.

10 Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the IT Consultant. No data to be stored electronically on physical media.

You should not store any personal data on any personal mobile device, only temporarily whereby the device belongs to the School.

Data may only be stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day by Automated Processing.

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.