Winchelsea

All Individuals Matter

WINCHELSEA PRIMARY SCHOOL
RUSKINGTON

INFORMATION HANDLING POLICY

June 2023

Introduction

Winchelsea Primary School recognises that all information required to deliver its services has value and therefore requires an appropriate degree of protection.

Adopting key principles and controls supports effective use of information, reduces information risk and assists the school in meeting its legal obligations.

Aim

The aim of this policy is to ensure that the confidentiality, integrity and availability of information is maintained by all staff.

Scope

This policy applies to:

- All information, regardless of format, processed by the school;
- Any individual processing information held by the school.

Sensitive Information

You must, at all times, ensure that care is taken when processing any school information.

Particular care must be taken when processing particularly sensitive information. Such information includes:

- Personal data and special categories of personal data as defined by the data protection legislation and as set out in the schools UK GDPR (Data Protection) Policy;
- Any other information that if subject to unauthorised access or amendment, or made unavailable, would cause a negative impact on the school's reputation, its finances, the services it delivers, or its staff, parents and/or pupils.

You must consider the nature and context of the information you are working with and exercise good judgement to ensure that school information is processed appropriately at all times.

General Principles

All information required to deliver services and conduct business has inherent value and therefore requires an appropriate degree of protection.

The confidentiality, integrity and availability of information must be respected at all times.

All staff processing information must take responsibility for ensuring it is subject to proportionate and reasonable controls relative to the sensitivity of the information and in a manner which reduces the risk to that information.

Information must be processed in a manner which meets legal and regulatory requirements including information received from, or exchanged with, external partners.

Staff must not access or attempt to access information for which they do not have an official purpose for accessing.

Personal data must be processed in accordance with the school's UK GDPR (Data Protection) Policy which supports its obligations under the current data protection legislation.

All staff processing information must undertake annual data protection training and be aware of their individual responsibilities.

Staff must not use private/personal devices to process sensitive information.

Handling and Storing Information

A clear desk (securing information when not in use) and clear screen (locking your screen when not in use) policy must be adopted at all times.

When not in use information, particularly sensitive information, must be stored securely e.g. under lock and key.

Access to information must be controlled at all times to ensure unauthorised access is prevented.

Information must only be removed from school premises when absolutely necessary and when doing so you must ensure it is protected in line with the requirements of this policy at all times.

Printed material must be collected from printers as soon as possible. Secure printing, which requires you to be physically present at the printer to receive the prints, must be used when the facility is available.

Information stored on portable ICT devices such as laptops and smartphones, or removable media, such as CDs and USB sticks must be encrypted.

Do not store information in an unoccupied vehicle. If it is unavoidable because more secure options are unavailable, then you must only store it out of sight in the locked boot of the vehicle. Information must never be stored in a vehicle overnight.

When discussing school business in public or by telephone, appropriate discretion must be exercised to protect information. Similarly, you must avoid being overlooked when working.

Before sending sensitive information ensure it is the minimum necessary to achieve your aim. For example, ensure you only share personal data with those who have a defined business need to see it and redact documents to remove unnecessary sensitive information.

When redacting information you must ensure it is achieved in such a way that prevents accidental disclosure of data. You must also carry out quality assurance checks before releasing the document to ensure redaction is successful.

Transmitting/sending Information

You must take care when transmitting/sending information to others.

By post/courier, you should use the tracked/signed for service via Royal Mail.

By email, you should type EncryptMail in the subject line to ensure the email is encrypted. When attaching documents ensure they are password protected.

Destroying Information

Hard copy information, such as files, letters, and plans must be securely destroyed when no longer required. This can be achieved by using a cross cut shredder.

If you intend to destroy information you must ensure access is controlled at all times until it is destroyed.

Hard copy information is not to be placed in open waste bins or waste skips.

Electronic information must be securely deleted from hardware/media when no longer required. Specialist advice is to be sought from Ark ICT Solutions Ltd.

Information Sharing and Disclosure

Information must only be shared with third parties when there is a legitimate and lawful purpose. All instances of information sharing that involves personal data should be documented.

Subject Access Requests, Freedom of Information requests and access to Education Records are to be directed to the school's Data Protection Officer – Mr Joe Lee.

Security Incidents

All security incidents involving information must be reported in accordance with the Security Incident Policy.

Further Information

For further information regarding information handling within the school please contact the Head Teacher.

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

Signed: _____ Dated: _____
Chair of Governors