Ashleigh Primary School and Nursery
Information Classification Guidelines

If you are reading a printed version of this document you should check the Information Management pages on the school website to ensure that you have the most up-to-date version.

If you would like to discuss anything in this privacy notice, please contact:

Data Protection Officer: dpo@dataprotection.education

If you would like a copy of any documentation, please contact the school office:

office@ashleigh.norfolk.sch.uk

Purpose

The purpose of this Guideline is to establish a framework for classifying, the appropriate handling and the use of data and information assets, based on its level of sensitivity, value and importance to the organisation.

Classification will aid in assigning security controls for the protection and use of data and information in order to ensure that data is created, stored, handled and destroyed appropriately to ensure controls can be put in place to make data available only to those authorised at any point during the data lifecycle.

Scope and definitions

This Guideline applies to all staff, pupils, governors and authorised third-parties (including parents) that create, access, process, or store Ashleigh Primary School and Nursery information assets. This applies to personal data and non-personal organisational data.

Information assets are digital and non-digital data created, processed, stored, archived, deleted while executing business activities. Examples are database records, emails, source code, paper documents, designs, emails, databases, Process Data, images etc.

An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organisation.

Irrespective of the nature of the information assets themselves, they all have one or more of the following characteristics:

- Information Asset is recognized to be of value to the organisation.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organisation’s corporate identity, without which, the organisation may be threatened.

Procedures

Data Classification

The classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

This classification system is designed to assist data owners *[a person assigned to be responsible for that data]* in assessing the data to determine the appropriate security controls for access, handling, storage, and destruction.

All organisation data and information must be classified into one of three sensitivity levels or classifications as soon as possible after the creation or transfer of ownership. The three levels are:

- Confidential
- Private
- Public

Classification should be the responsibility of the document owner or other authorised individual.

Definition	Confidentiality	Integrity	Availability
Public	Non-sensitive information is available for public disclosure. The impact of unauthorized disclosure **does not harm the organisation**. E.g. Newsletters or information published on the school website	There is **minimal impact** on business if the accuracy and completeness of data is degraded.	There is **minimal impact** on business if the asset / information is unavailable for up to 7 days
Private	Information belonging to the organisation and not for disclosure to public or external parties. The unauthorized disclosure of information here can cause a **limited harm** to the organisation. e.g. Organisation charts, Internal Telephone Directory.	There is **significant impact** on business if the asset if the accuracy and completeness of data is degraded.	There is **significant impact** on business if the asset / information is not Available for up to 48 hours
Confidential	Information, which is very sensitive or private, of highest value to the organisation and intended to use by named individuals only. **The unauthorized disclosure of such information can cause severe harm** (e.g. legal or financial liability, reputational damage). E.g. pupil safeguarding data, employee payroll data	The Integrity degradation is **unacceptable**.	The Asset / information is **required on 24x7 basis**

Definition

Confidentiality
Confidentiality of information refers to the protection of information from unauthorized disclosure.

The impact of unauthorized disclosure of confidential information can range from jeopardizing organisation security to the disclosure of private data of students or employees.

Integrity
Integrity refers to the completeness and accuracy of Information. Integrity is lost if changes are made to data or IT systems by either intentional or accidental acts, or if data is not up-to-date and accurate. If integrity of data is not maintained, continued use of the contaminated data could result in inaccuracy, fraud, or erroneous decisions.

Availability
Availability indicates how soon the information is required, in case it is lost or access disrupted. If critical information is unavailable to its end users, the organisation's mission may be affected.

Labelling

All data or information in electronic or hardcopy format that is not Public information must be labelled as Confidential or Private

Confidential:

- Individual documents with multiple pages should be labelled on each page (usually in the header, footer or watermark of a standard office document).
- Emails should have a classification statement as the first statement of the email.
- Where the data is not in a document format, efforts should be made to indicate or control the data classification

Private:

- Individual documents with multiple pages should be labelled on each page (usually in the header, footer or watermark of a standard office document).
- If not labelled, internal communications and documents should be assumed to be Private

Public documents have no specific labelling requirement

Collections of Data

Organisations may wish to assign a single classification to a collection or group of data, especially where the data is of a common type. For example, all the content within a personnel or safeguarding file.

Also, due to storage limitations, data may be stored in locations with other types of data.

In these circumstances, all data in the collection or location should be classified at the most restrictive classification or assigned the highest level of access control.

When considering a collection of data, bear in mind that the aggregated data may result in a collection of data that requires a higher classification than any individual information asset. For example, an individual teacher's appraisal may be classed as Private, but a set of all teachers appraisals may be considered Confidential.

Data Safeguards

The Organisation and the owners of the information assets are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, labelling handling of, storage of, transmission of, and disposal of print and electronic data.

Transmission

Transmission is the movement of data.

Confidential and Private data when transmitted externally should be sent via secure email or using encrypted and secure devices. Where possible, include data in a document and share this document using access control, rather than attaching as an email.

When sent physically, it should be sent via secure and recording postage or courier.

Destruction

Data should be destroyed according to its importance:

Confidential and Private data:

Securely shred immediately, or place into locked secure containers until securely destroyed. Use of shredding bags without securing them (placing in locked cupboards) is considered insecure and breach of the confidentiality requirements of this document.

The organisation's IT Manager should implement procedures and technical measures for the secure destruction of electronic data and physical hardware.

Public data:

Can be placed in open recycling containers.

Compliance

Non-compliance to this Guideline may result in disciplinary action.