
*At Ashfield Valley we care for and value every child in a nurturing, inclusive environment.*
*All members of our school community will work hard to ensure that every pupil achieves their full potential and has the opportunity to shine.*

# Overarching IG Policy

Reviewed: September 2022
Date of next review: September 2023

# 1. Summary

Information is a vital asset and resource, both in terms of the management of individuals and the efficient management of services and its support. It plays a key part in governance, planning and performance management. Information Governance brings together the requirements and standards of practice in relation to the following areas:

- Data Protection
- Data Quality
- Freedom of Information
- Information Security
- Information Sharing
- Records Management

Implementation of this policy will contribute significantly towards assuring School stakeholders that information is being processed in compliance with legislation and Policies. This policy will support the provision of high quality services by promoting the effective and appropriate use of information.

# 2. Introduction

Ashfield Valley Primary School is committed to protecting the privacy of individuals and handles all information in a manner that complies with relevant legislation & codes of practice including but not limited to the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000 and common law duty of confidentiality. The School has established this policy to support that commitment.

The Policy applies to all information held on paper or in electronic format including recorded information e.g. CCTV, voice recordings.

Everyone managing and handling information, particularly personal information, needs to understand their responsibilities in complying with the legislation & codes of practice. It is the personal responsibility of:

- All employees of the School
- All employees and agents of other organisations who directly or indirectly support the School
- Those engaged on interim contractual arrangements or agency contracts working on behalf of the School

The School recognises that there are risks associated with managing information in order to meet legislative and other requirements. This policy is intended to facilitate compliance & reduce risks and all staff should be aware of its content and requirements.

The School has a clear commitment to ensuring that all staff have access to appropriate training and guidance. Staff managing and handling personal & other information will be adequately trained.

The School has access to appropriately qualified and experienced IG resource.

# 3. Policy

## 3.1 Data Protection

The Data Protection Act 1998 (DPA 1998) regulates how an organisation can use (process) personal information about individuals. The School has established this policy to ensure it meets the requirements of the Act and has clear procedures and arrangements in place to manage compliance across all areas.

The School is registered as a 'Data Controller' with the Information Commissioners Office (ICO). A Data controller must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, prosecution, and compensation claims from individuals.

The School has a Privacy Notice in place. The Data Protection Act requires the School to process personal data 'fairly'. The Privacy Notice ensures that individuals are aware of how the School use their personal information. This is supported in other ways to tell pupils and parents how their information will be used e.g. forms and other information such as leaflets/notices.

The policy supports the rights of individuals (data subjects) who wish to see information the School holds about them (by submitting a Subject Access Request).

## 3.2 Information Security

Information security is the practice of protecting information from unauthorised access, modification & use. The School has effective safeguards in place to make sure that personal and other information is kept securely and does not fall into the wrong hands. The School has clear procedures and arrangements to manage the human and technical elements of Information Security.

The School will maintain & protect all information assets to a high standard of confidentiality, integrity and availability. The School will ensure that information assets and hardware are disposed of securely in line with industry standards.

Important information assets will include paper records stored on or off site, computers, mobile phones, emails, data files, software, recorded information e.g. CCTV, voice recordings.

The School will ensure that any security incidents that occur are managed in line with available procedures for Information Security Breach.

## 3.3 Data Quality

Consistent, high-quality, timely and comprehensive information is vital to support good decision-making, protect vulnerable people, improve outcomes for pupils and reduce unnecessary work. Information is a vital asset and resource, both in terms of the management of individuals and the efficient management of the School. Data must be fit for purpose and accurately represent the organisation's activity. Data quality measures promote the principle of 'getting it right the first time'. The School is committed to identifying and promoting good practice.

Data quality is the responsibility of every member of staff collecting data or entering, extracting or analysing data from any of the School information systems. All staff members should know how their day-to-day job contributes and how lapses can affect, the Schools reputation, financial penalties/fines, performance management, delivery (particularly to vulnerable people) & the allocation of funding to the School.

## 3.4 Records Management

The School will ensure appropriate arrangements are in place for the care and management of its records to meet its legal and regulatory requirements. School records will be accurate and accessible, giving a fair and truthful representation of the work and processes undertaken.

The School will manage records throughout their lifecycle from creation to eventual disposal thus ensuring that records are complete, authentic, trustworthy and secure and are available when needed. The School has clear procedures and arrangements for handling records including a Retention Schedule.

The School recognises that there are risks associated with managing records in order to meet the requirements of the Act. This policy is intended to mitigate those risks.

### 3.5 Information Sharing

The School will ensure that it is mindful of the legal basis for sharing data including personal data with external partners especially in relation to non-routine data sharing or new projects where the sharing process changes in terms of purpose, parties, type of data, or means of sharing i.e. new computer systems etc. (the why, who what and how).

The School will ensure that in all cases where consent of an individual is required that the requisite privacy notices are given to individuals to enable them actively to give informed consent.

The School will use a range of Contractual terms, Data Processor and Information Sharing Agreements as may be appropriate to manage the sharing and disclosure of information to bodies within and outside the School.

Privacy Impact Assessments will be used to assess and mitigate risks identified and support good information sharing practice.

### 3.6 Freedom of Information & Environmental Information Regulations

This policy has been established to ensure that the School meets its legal obligations under the Freedom of Information (FOI) Act. It outlines the approach to responding to requests for information made under the FOI Act. The School is committed to openness and transparency about the way in which it operates.

This will be balanced against the need to ensure the confidentiality of certain information, in areas such as personal information and commercially sensitive information. Information of this type will be redacted (removed) prior to release.

The Freedom of Information Act (FOIA) gives any member of the public the right of access to information held by the School about how it runs the business. It does not include access to personal information (information that identifies a living individual) which is dealt with under the Data Protection Act. Nor does it include access to Environmental Information (see below)

The School will have clear procedures and arrangements for handling queries from members of the public.

The School recognises that there are risks associated with providing information in order to meet the requirements of FOIA. This policy aims to mitigate the following risks:

- Not providing requested information within the statutory 20 days.
- Providing information that should not be in the public domain e.g. personal information, commercially sensitive information etc.
- Not providing information that should be made available leading to Internal Reviews and ICO complaints, putting strain on School Resources.

The School will also provide access to environmental information through the Environmental Information Regulations 2004 (EIR). These regulations set out an access regime that is broadly similar to the FOI Act. There are some small, but significant differences with the EIR, especially in terms of exceptions from the right of access and charging for information provided. In general EIR encourages the provision of information and there is less scope for refusal to provide it.

## 4. Process for Monitoring Compliance and Effectiveness of the Policy

## Document

Information Governance is viewed seriously by the School. Any breach of this Policy and other associated requirements, will be considered or investigated under both the School Disciplinary Procedure and Information Security Breach Procedure or restricted to one of the two procedures. The incident could lead to legal or regulatory action being taken against the school. The outcome of investigations may result in disciplinary action which may have serious consequences for an employee's continued employment.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Section 55 of the Data Protection Act 1998 makes it an offence to obtain, disclose or 'procure the disclosure' of confidential personal information 'knowingly or recklessly', without the consent of the organisation holding the data. Examples of a Section 55 offence include: misusing School systems to source information for personal use, 'hacking' of School systems, selling personal data held on a School system.

Section 77 of the Freedom of Information Act 2000 makes it an offence for any person to deliberately alter, deface, block, erase, destroy or conceal a record after it has been requested with the intention of preventing its disclosure.

Serious violations will be considered gross misconduct and as such may lead to the dismissal of the employee or employees concerned.

## 5. Glossary of Terms

| Term | Meaning |
|---|---|
| Data Protection Act 1998 | The main piece of legislation that governs the protection of personal data and privacy in the UK. |
| Human Rights Act 1998 | Article 8 covers the right to respect for family, private life, home and correspondence and makes it unlawful for any public body to interfere with that right. |
| Privacy Impact Assessments | A tool to identify and address privacy risks for projects or changes in practice. |
| Freedom of Information Act 2000 | The main piece of legislation providing public access to (non-personal) information held by public authorities. |
| Environmental Information Regulations 2004 | Covers access to environmental information held by public authorities. |