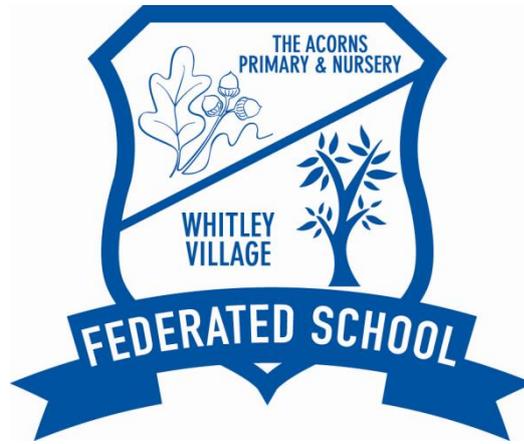


THE ACORNS PRIMARY and NURSERY and WHITLEY VILLAGE
FEDERATED SCHOOL



DATA PROTECTION POLICY

April 2017

The Acorns Primary and Nursery and Whitley Village Federated School

Introduction

The processing of personal data is essential to many of the services and functions that the School carries out. The Acorns Primary and Nursery and Whitley Village Federated Schools complies with Data Protection Act 1998 in order to process data fairly and lawfully, in line with the Eight Principles and with respect to all sections of the Act. This policy sets out how the School will comply with the Data Protection Act 1998 and the Human Rights Act 1998 in order to respect the rights of the individual whilst also providing appropriate services to the public.

1 Purpose

The purpose of this policy is to define the School's responsibilities and reassurances under the Act. This policy is designed to give staff an overview of how the Data Protection Act impacts on their roles within the School and aims to inform their decisions and day to day work by providing a legal background to the Act.

2 Scope

This policy applies to all employees, governors and partner agencies who:

- Process personal data as part of their role or on behalf of the School.
- Access systems of a sensitive nature.
- Have access to buildings where personal data is stored.

3 Policy Statement

This policy sits beneath the School's overarching Information Security Policy (ISP01) and will link in with the Council's Information Sharing Policy and Procedure (ISP24, ISP24a).

The policy provides a reference point for all staff when handling personal data and highlights the underpinning principles of the Act that govern all of the School's processing of personal data.

3.1 Definitions

Personal Data – is data that can be used to identify any living individual either on its own or in conjunction with other data. Examples of this include names, dates of birth, addresses.

Sensitive Personal Data – is data that can disclose the following about a living individual

- Their race
- Their religion
- Their political opinions
- Their sexual life/orientation
- If they are a member of a Trade Union
- If they have a physical or mental health condition
- If they have a criminal record or have been linked to any offences

Processing Personal Data – is essentially any action involving personal data, this can include storing, sharing, creating, altering, organising or deleting. It is not limited to these examples and applies to both physical and electronically held data.

Data Subject – is an individual who is the subject of personal data.

Data Controller – is a person or organisation who decides the purposes for processing personal data. The Acorns Primary and Nursery and Whitley Village Federated Schools is a data controller. All schools are data controllers.

3.2 The Eight Principles

The Data Protection Act can be summarised in eight principles that apply to the way the School processes personal data across all of our functions. The principles ensure that personal data is: -

1. Processed fairly & lawfully, where necessary applying a Schedule 2, and in the case of sensitive personal data, a Schedule 3 condition (schedule 2 and 3 conditions are detailed in ISP24a)
2. Processed only for a specified purpose and not processed for any purpose incompatible with the original purpose.
3. Accurate, relevant and not excessive
4. Accurate and up to date
5. Not kept longer than is necessary
6. Processed in accordance with the rights of the data subject
7. Stored securely with appropriate physical and technical security measures in place
8. Not transferred outside of the European Economic Area (EEA)

3.3 Conditions

When processing personal data, the School will always apply the appropriate Schedule 2 condition. When processing sensitive personal data, as defined in Section 2 of this policy, the School will also apply an appropriate Schedule 3 condition as well.

3.4 Individual's Rights

Under the Sixth Principle of the Act, the individual data subject is granted a number of rights.

- A right of access to a copy of the information comprised of their personal data
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.
- A right to claim compensation for damages caused by a breach of the Act.

The Acorns Primary and Nursery and Whitley Village Federated Schools is dedicated to upholding the rights of the individuals as set out in the Act.

3.4.1 The Right of Access (Subject Access Requests)

The School has a dedicated team that handles Subject Access Requests. A request must be made in writing, either using the physical SAR form or electronically via email. It must also be accompanied by proof of identity, proof of address (if the applicant requires information in the post) and a ten-pound fee. The School must provide all information held about the applicant (subject to exemptions) within forty days of receiving the complete request, as dictated by the Act.

The School has a Subject Access Request Procedure which reinforces the School's commitment to upholding the right of access and details the process of preparing information for release. [Link to this and to the ICO Code of Practice.](#)

3.4.1.1 Upholding the rights of the individual

Where an individual data subject, either a member of the public or a member of staff, has a question or complaint regarding how their rights under the Act are upheld, they are encouraged to make contact in writing (or email) to the Information Governance Team in the first instance using the contact details below.

Email – dpawest@cheshirewestandchester.gov.uk

Phil Orchard - Data Protection Officer
Data Protection Team (2nd Floor, HQ)
4 Civic Way
Ellesmere Port
Cheshire
CH65 0BE

Data subjects who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased. They will receive a written response indicating whether or not the School agrees and if so, the action to be taken. In the event that the School disagrees, the data subject may request their objection be recorded with the relevant record.

A notice may be served by the data subject objecting to the processing and/or way in which the information is being processed, and requesting the School to cease doing so on the ground this may cause substantial unwarranted damage or distress to the data subject. A written response indicating the School's intentions will be given within 21 days of receiving the request. This will explain whether or not the School intends to comply with the request, including any parts of the request which the School considers unjustified.

Data subjects may ask the School for an explanation of any decision likely to significantly affect them which has been, or may be, taken solely by wholly automated means. The School will consider a request that a decision which significantly affects an individual is not based solely on automated means and consider reviewing a decision which has been taken, or, consider taking a new decision on a different basis, in circumstances where either course of action is appropriate and timely, unless the automated decision qualifies as an exempt decision.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be dealt with under an appropriate internal complaints procedure, or, in the case of an employee through the School's grievance process.

Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

3.5 Legal Requirements

The School may receive requests for information from various sources. This can include court orders, or requests under Section 29 (Crime & Taxation) or Section 35 (Legal Proceedings).

All external agencies, contractors or Service Level Entities (SLEs) that the School engages with must demonstrate the technical and legislative ability to uphold the principles of the Act and the rights of the individual when handling or receiving School owned personal data.

The School will write, uphold and regularly review Information Sharing Agreements (ISAs) when sharing information on a data controller to data controller basis. The School will ensure that appropriate contracts and data processing agreements are in place when using third party contractors as data processors. All of the School's data sharing and data processing arrangements are written in line with the ICO's Data Sharing Code of Practice, ICO's guidance on the role of Data Controllers and Data Processors and the School's Information Sharing Policy.

The School reserves the right to monitor telephone and email correspondence and internet usage, in line with relevant legislation. This will be handled with respect of all guidance from the Information Commissioner's Office.

4 Responsibilities

The Information Governance Strategy Group (IGSG) is responsible for ensuring compliance with this policy and overall information governance across the School.

The School will ensure that all employees responsible for handling personal data will receive appropriate training in the use and control of this data. School staff responsible for sensitive personal data will also receive training appropriate to their roles.

The School will implement a process to ensure all staff handling personal information know when and how to report any actual or suspected data breach, and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

The School will monitor and review its processing activities to ensure these are consistent with the principles of Data Protection legislation and will ensure that its notification is kept up-to-date.

The School will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that appropriate Privacy Notices are maintained to inform data subjects of how their data will be used.

The School will review and update this policy to ensure it remains consistent with the Law, and any Compliance Advice and Codes of Practice issued by the ICO.

5 Compliance with legal and contractual obligations

This policy is written in accordance with the Data Protection Act and the associated guidance from the Information Commissioner's Office. All staff have a duty to act responsibly and in reference to the Act when handling personal data. All School employees, elected members, contractors and agency staff have a duty to educate themselves regarding their responsibilities under the Act and how to mitigate the risk of a breach.

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to School assets, or an event which is in breach of the School's security procedures and policies.

All employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the School's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the School.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the School's ICT systems or network results from the non-compliance, the School will consider legal action against the third party. The School will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process. Elected members may be referred to the standards agency.