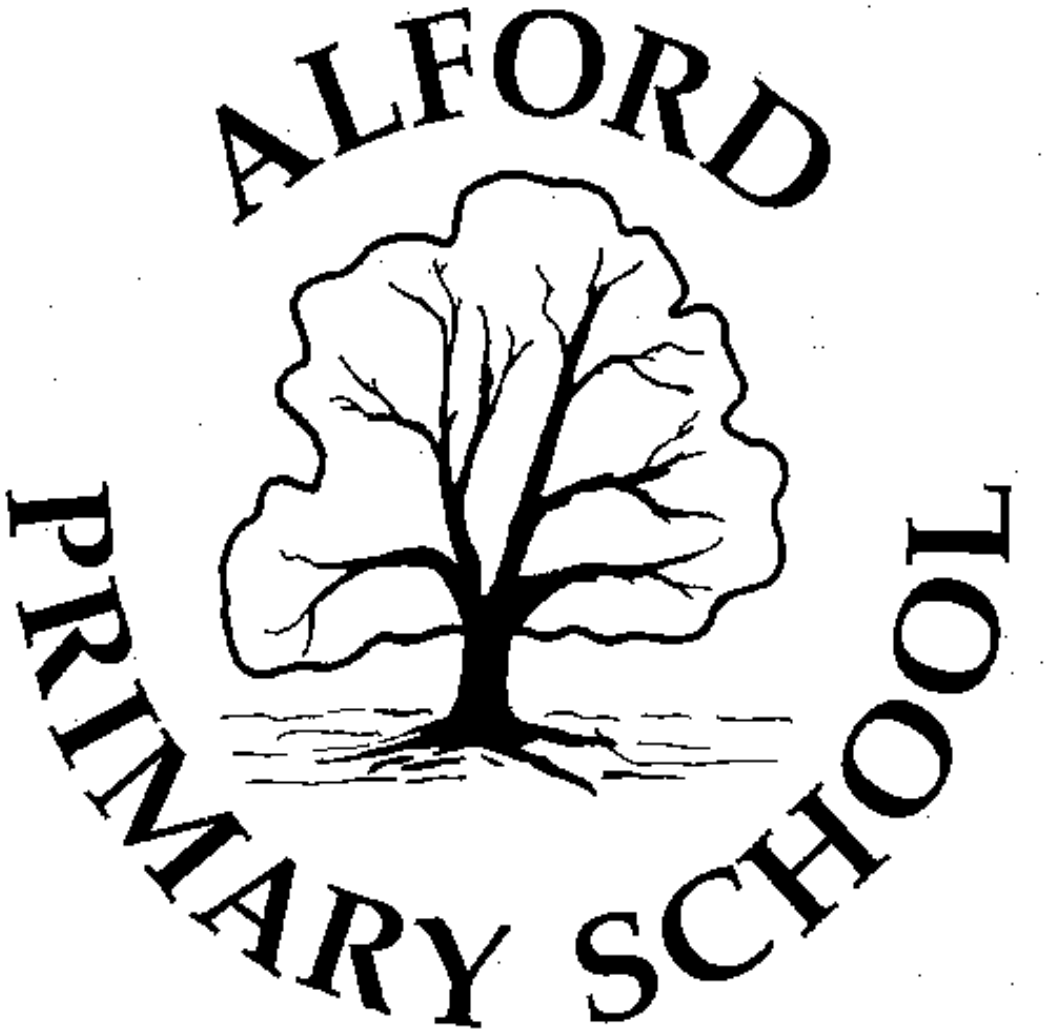

DATA PROTECTION & INFORMATION SECURITY POLICY

Reviewed Annually by the Fabrics Committee

Date of last Review	Signature
Spring 5th March 2018	Chair:

Data Protection Policy

Alford Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Alford Primary School needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

For the latest changes and more information, please see the Privacy Notice available on the School's website.

In summary, these principles state that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

All staff who process or use personal information, must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The School, as a body, is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has identified its Designated Data Controllers as: the Headteacher, Deputy Headteacher, the Business Manager and the Business Support Staff.

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child, should raise the matter with the Headteacher, in the first instance.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided eg. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- Handling all personal data (eg. pupil attainment data) with reference to this policy.

Information Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidently or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a filing cabinet, drawer, or safe in a secure office, or;
- If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a USB memory key or other removal storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The School will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

The School may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Retention of Data

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time. (See Records Management toolkit in the office).

Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed, the policy will be amended at its next review.

1. Information Security Policy Statement

Alford Primary School recognises information as an important asset of significant value to the organisation. It also recognises the need to protect information and to ensure it is processed in a secure manner. This will be achieved by:

1. Ensuring the confidentiality, integrity and availability of information and information assets belonging to the school and entrusted to us by members of the public, our strategic partners, and other third party organisations;
2. Adopting an Information Security Management System (ISMS) which considers a diverse set of security controls aligned to ISO/IEC 27001:2013;
3. Continually improving the ISMS by measuring the effectiveness of controls and adapting to new and emerging risks;
4. Maintaining compliance with relevant UK and European Union legislation e.g. Data protection legislation;
5. Establishing information security objectives to improve information security performance;
6. Ensuring effective policies and procedures are in place to support secure working practices;

7. Educating and training staff to handle and process information securely;
8. Ensuring specialist staff are available to provide support and guidance;
9. Investigating and recording all actual and suspected security incidents.

2. Scope

This policy applies to:

All information, regardless of format, processed by the school;

All information ICT infrastructure and services operated or managed by the school;

It is supported and approved by the school's Chief Executive, Senior Information Risk Owner, and Corporate Management Board.

3. Impact of Failing to Safeguard Information

3.1. The school recognises that failing to safeguard information can have varying degrees of impact depending on the type of failure and the information involved. It includes:

Undermining of public confidence in public services;
Negative impact on public finances;
Embarrassment or distress caused to parents, pupils or staff;
Reduced effectiveness in the performance of business activities;
Failure in the provision of school services; and
Reputational damage.

4. Access Control Principles

1. Access must be strictly controlled in order to maintain the confidentiality, integrity and availability of information and systems.

2. The overall security of the infrastructure, systems, and information must take precedence over any individual requirement for access.

3. Access rights must be based on a clear business need and must be afforded in line with the principles of need to know and need to access.

4. The allocation and use of privileged access rights must be strictly controlled.

5.. Access to the School Network must be through the provision of a unique User ID which must be assigned to an individual user to enable an audit of specific activity and to ensure accountability of actions.

6. Generic user accounts must not be permitted unless exceptional circumstances exist and only when there is a clearly defined and documented business reason to do so.

7. Account holders must conform to the school's E-Safety & Acceptable Use Policy.

8. Access provided to non-school staff must be supported by a relevant information sharing agreement and/or contract which sets out appropriate information assurance requirements. Services must be the minimum necessary.

9. Access to school email must be strictly limited to school staff or those representing the school.

5. Access Authorisation

Before access is authorised a formal process must be followed which requires that:

1. An agreed business need is identified.
2. Authority is provided by a relevant line manager.
3. The identity of the User is verified.
4. The provision of privileged access is via formal change control.
5. The level of access provided must be commensurate with the tasks the User is expected to perform.
6. Users must change their passwords at the first log on.

6. Adjustment of Access Rights

1. Adjustments to access rights must be based on the criteria set out at Para 4.
2. Access rights to systems used by staff when changing roles must be reviewed by managers and updated where necessary e.g. removal of unnecessary access permissions within IMP.
3. Suspension of access rights must be requested by the relevant Line Manager for lengthy periods of planned inactivity e.g. secondment; suspension; maternity leave; long term sick leave.

7. Disabling of User Accounts

1. Once a business requirement ceases to be relevant e.g. due to contract termination, staff transfer, resignation, or retirement, access to the school network and to systems previously required to complete a role must be revoked and the users account disabled.
2. Line Managers are responsible for notifying the IT Service Desk of the need to disable the User account and to disable any access permissions the user had to systems used as part of their role.
3. ICT assets must be recovered from employees once a business requirement has ceased and returned to school.

8. Allocation of Privileged Access Rights

1. The allocation of privileged access rights must be strictly controlled and must follow the access authorisation process.
2. Privileged access rights must be consistent with an individual’s role.

3. Privileged access rights must be subject to formal change control process.
4. Privileged access rights must be assigned to a User ID different from those used for regular business activities. Regular business activities must not be performed from a privileged ID.
5. When privileged access rights are no longer justifiable they must be removed as soon as practicable.
6. A regular review of privileged access rights must be undertaken (not less than once every six months).
7. Users requiring administrative privileges (for example, users who are able to reconfigure the network or system administrators) must be subject to the Baseline Personal Security Standard.

9. Supporting Policies

1. This policy statement is supported by a number policies, procedures and standards. Those information security policies which staff need to have an understanding of are E-Safety & Acceptable use policy and Information Risk Management Policy & its relevant toolkit.

2. The policies will be made available to all staff electronically and can be accessed via the school's external website.

3. The policies support a layered approach to protecting information and information assets. This refers to the application of a number of different security controls rather than relying on a single control.

4. In addition the school will ensure it provides and maintains an appropriate policy set designed to support information processing, for example a Data Protection Policy and Records Management Policy.

10. Compliance

1. School employees have a contractual responsibility to be aware of and conform to school values, rules, policies and procedures. Breaches of policy may lead to the employee going through the school’s disciplinary procedure in accordance with the Code of Conduct and the school's disciplinary policy.

2. Individuals who are not school employees and who fail to comply with school policies may have their access to school information and ICT revoked and such action could have an impact on contracts with third party organisations.

11. Further Information

For further information please email IT.Service@alford.lincs.sch.uk


Information Security Policy Statement
Provides the council's information security policy statement.
Information security roles
Identifying information risk
Assessing information risk
Treatment of information risk
Monitoring information risk
Information Risk Management Policy
Sets out individual responsibilities when accessing council ICT and information including:
Training and awareness
General Responsibilities
Unacceptable Use
Email
Passwords
Removable media
Remote working
Monitoring
Breaches of policy
Acceptable Use Policy
Information classification
Categories of sensitive information
General principles
Handling and storing
Transferring
Information Sharing
Destruction
Information Handling Policy
Physical Security Policy
Building security
Room security
Visitor access
Personal identification
Security of ICT assets
Principles of access to the council's network
Network access authorisation
Privileged access rights
Audit and review of network accounts
Dormant accounts
User Access Control Policy
Security Incident Reporting Policy
Definition of a security incident
General principles
Actions on identifying a security incident
Managing an incident
Internal & external reporting
Third party security controls in:
Protecting electronic/hardcopy data
Electronic data transfer
Network Security
Security incident reporting
Minimum Security Controls – third party information sharing / processing