DATA PROTECTION POLICY

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer, who may be contacted via the school office.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller

- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Head teacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the school office.

Appendices

1. Privacy Notice (Published on website)
2. Information for Staff and Governors
3. Staff agreement (to be filed in personnel records)
4. Checklist for Obtaining Consent
5. Consent template form
6. Information Audit
7. HCC Retention Schedule
8. Subject Access Request Checklist
9. Subject Access Request Guidance
10. Data Protection Impact Assessment Guidance and Form
11. Data Breach Initial Reporting Form

Drafted by J Dunlop

Policy to be reviewed every two years.

Policy to be the responsibility of Resources Committee

Approved by the Governing Body	/ /

Chair of Governors signature Date	…… / /

Review date	/

APPENDIX A
CONFIDENTIALITY POLICY

MISSION STATEMENT

We are growing together on our journey of achievement with Jesus in our hearts, heads and hands.

POLICY STATEMENT

Working in St. Joseph's Catholic Primary School necessarily means having access in a variety of ways to information that must be regarded as confidential. Therefore, this policy applies to all staff employed by the school, including temporary, voluntary and agency staff. It also applies to governors, volunteers, visitors on work experience placements and parent helpers.

TYPES OF CONFIDENTIAL INFORMATION

Information that is regarded as confidential can relate to:

1. A variety of people e.g.

- pupils;
- parents;
- staff/colleagues;
- governors;
- job applicants.

2. A variety of matters, e.g.

- home addresses & telephone numbers;
- conduct and performance;
- performance & development review/performance management;
- health/medical;
- pay and contracts;
- references;
- internal minutes, memos etc.;
- confidential budgetary or policy information;
- other personal information.

These lists are not exhaustive but will extend to cover any other information of a sensitive nature relating to employees, pupils and others connected with the school and to the work of the school itself.

POTENTIAL RECIPIENTS OF INFORMATION

Within the course of daily operation, information related to the school, or those connected to the school, may be requested by, or supplied by, or passed to a range of people.
This might include:

- internal colleagues (teachers, support staff, governors);
- colleagues in other schools;
- management teams;
- pupils;
- governors;
- trade unions/professional associations;
- parents;
- partner organisations (LA, DfE, Teachers' Pensions);
- other external organisations;
- the public;
- the press;
- contractors/potential contractors.

Great care must be taken by both the recipient and the supplier of information to ensure that it is dealt with in a sensitive manner.

Particular responsibilities

- If someone requesting information is not known to staff, particularly in the case of telephone calls, his/her identity and the legitimacy of his/her request should be verified by calling them back. A person with genuine reasons for seeking information will never mind this safety measure.
- Wherever possible, a response to requests for information should only be given when the request has been made in writing e.g. employee references.
- The same principle applies when sending Emails. Staff should always check that the information is going to the correct person and is marked confidential where appropriate.
- **Being known as an employee of the school may mean being asked for information, for instance, by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential school matters.** Persistent enquiries should be referred to the Headteacher.
- The Data Protection Act refers to the principle of third party confidentiality. Information relating to, or provided by, a third party should not be released without the written consent of the third party or unless an order for disclosure is made by a court of competent jurisdiction.

Where they are unsure what to do, staff should refer the matter to the Head teacher or, in her absence the deputy head teacher, for guidance.

THE FORM CONFIDENTIAL INFORMATION CAN TAKE

Confidential information can take various forms and be held and transmitted in a variety of ways, e.g.

- manual records (files);
- computerised records, flash drives/ memory sticks;
- written reports/minutes/agendas/file notes etc.;
- letters, memos, messages;
- telephone calls;

- face-to-face;
- Email;
- Internet.

THE METHODS OF ACQUIRING INFORMATION CAN ALSO VARY

Individuals and groups may become aware of confidential information in the following ways:

- access is gained as part of the employee's day to day work;
- information is supplied openly by an external third party;
- employees may inadvertently become aware of information;
- information may be disclosed.

Particular responsibilities

- Employees should be aware that they may have disclosed to them sensitive information in the course of their work or outside. In some circumstances the individual may request that the information remains confidential.
- Staff will also need to be aware that they may be obliged to disclose certain information e.g. relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or direct them to a more appropriate officer or decline to receive the information. Employees should use their discretion regarding these matters, should refer to appropriate procedures and, if in doubt, should seek advice from the Head teacher.

RESPONSIBILITY OF INDIVIDUALS IN POSSESSION OF SENSITIVE INFORMATION

All information received in the course of employment, no matter how it is received, should be regarded as sensitive and confidential. While it is often necessary to share such information, in doing so, employees should consider the following key points.

1. The nature of the information:
   - how sensitive is it?
   - how did it come to your attention?

2. The appropriate audience:
   - who does the information need to be shared with?
   - for what purpose?
   - who is the information being copied to? Why?
   - does restriction of access need to be passed on to your audience?

3. The most appropriate method of communication:
   - verbal;
   - written;
   - Email;
   - in person.

4. The potential consequences of inappropriate communication.

It is also an individual employee's responsibility to safeguard sensitive information in their possession.

Particular responsibilities

1. Sensitive information should be kept secure.

- Filing cabinets should be kept locked when unattended.
- Child protection information is kept in a separate, secure locked cupboard.
- **Sensitive information should not be left on desks or the photocopier/printer.**
- **Papers should not be left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, precautions must be taken to ensure that they are not accessible to third parties.**
- Appropriate steps should be taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipients name and position.
- If it is necessary to supply personal files through the external mail, this must be sent by recorded delivery.
- Copies of emails should be stored securely.
- Steps should be taken to ensure that private/confidential telephone calls/ conversations are not overheard.
- Meetings where sensitive or confidential information is being discussed should be held in a secure environment.
- Confidential paperwork should be disposed of correctly either by shredding it or using the confidential waste bags stored in the school office.
- Personal data should not be used for training or demonstration purposes where fictitious data can be used.

2. Computer data should not be left exposed to others' view when unattended.

- Screen savers should be used when computers are unattended.
- Machines should be switched off overnight.

3. Computer files should be kept securely.

- Passwords should be used and these should not be disclosed to colleagues unless absolutely necessary.
- Passwords should be changed periodically (at least every 6 months).
- Sensitive data should not be stored on public folders.
- Staff should be familiar with the security of Email/internet systems.
- Staff should use the school email service for all school related emails
- Access to individual's computers should be restricted.
- Any user Ids and passwords used for the internet should remain confidential.
- All work carried out on a computer should be stored safely either in a personal directory, or onto a memory stick or portable hard drive which should be kept securely.
- Computer files should backed up regularly and not solely saved to the hard disk.

4. A variety of phrases may be used on correspondence to denote confidentiality. As a general rule:

- Post marked 'personal' or 'for the attention of the addressee only' should only be opened by the addressee personally;
- Post marked 'private' and/or 'confidential' may be opened by those responsible for distributing the post within the school.

5. Confidential mail which is then forwarded internally should continue to carry a confidential tag.

Other responsibilities

- Employees should have regard to potential difficulties which may arise as a result of discussions outside work. While it is natural (and indeed can be therapeutic) to talk about work at home or socially, staff should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Staff should be particularly aware that many people have a direct interest in education and schools and even close friends may inadvertently use information gleaned through casual discussion.
- Personal (e.g. home addresses and telephone numbers) and work-related information (e.g. salary details, medical details) relating to individuals, should not be disclosed to third parties except where the individual has given their express permission (e.g. where they are key holders) or where this is necessary to the particular work being undertaken, e.g. it is necessary for an individual to be written to.
- The Headteacher should comply with the procedures for the storage and sharing of information relating to individuals' Performance Management Appraisal Reviews.
- Personal and case files should not normally be shared with third parties other than the Deputy Head teacher and those responsible for writing references. Exceptions may apply in the case of legal proceedings.

Employees should use their discretion in these matters and if in doubt, should seek advice from the Headteacher.

THE CONSEQUENCES OF REVEALING CONFIDENTIAL INFORMATION WITHOUT AUTHORITY

Staff should ensure that they are familiar with this Confidentiality Policy and related Policies. While there is an expectation that staff will use their professional discretion in applying the Policy, they should always seek advice from the Headteacher where they are unsure.

Staff should be aware that serious breaches of the Policy may result in disciplinary action being taken. The severity of the sanction will be assessed with regard to the potential harm the disclosure will have caused to the individual concerned. Some breaches of confidentiality could be regarded as potential serious or gross misconduct that could result in dismissal.

Policy drafted by J Dunlop.
This policy is to be reviewed every 5 years.
Policy to be the responsibility of the Resources Committee

Approved by the Resources Committee at its meeting on:	
Chair of Resources Committee signature: Date:	
Review date:	