Trinity St Mary's Church of England Primary School

Confidentiality Policy

Summer Term 2023

"Many Hearts Make A School"

We work together to teach and inspire our children so that they have the confidence to flourish in our community and in the world.
Like the wise man who built his house upon the rock (Matthew 7:24-25), we embrace our Christian values to build strong foundations for their future.

Introduction

Working in the school environment 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 and visitors on work experience placements.

The Confidentiality Policy outlines:

- the various types of confidential information which exist;
- the potential recipients of information;
- the form confidential information can take;
- individual responsibilities of staff in possession of confidential information;
- the potential problems that can arise and how to deal with them;
- the consequences of revealing confidential information without authority.

Staff should also have regard to relevant aspects of the following policies where these have been adopted by the Governing Body.

- Code of Conduct.
- Whistleblowing.
- E-Safety.
- Child Protection.
- Safeguarding.
- Anti-Bullying.
- Behaviour for Learning.
- Data Protection.

Types of Confidential Information

Information that is regarded as confidential can relate to a variety of people, for example:

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

And a variety of matters, for example:

- home addresses and telephone numbers;
- conduct and performance;
- performance and development review/performance management;
- health/medical;
- pay and contracts;
- references;
- internal minutes, memos etc;

- confidential budgetary or policy information;
- behaviour and child protection information;
- other personal information.

These lists are by no means 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 business or those connected with it, may be requested by, supplied by, or passed to a range of people. This might include:

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

Clearly, the sensitivity of the information will be partly dependent upon the recipient/supplier and the manner in which it is transferred. 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.
- It is a requirement under the Data Protection Act that action is taken to ensure the validity of any caller even if they state they have a statutory right to the information requested.
- Wherever possible requests for information should be 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 can 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 Headteacher or line manager for guidance.

The form confidential information can take

Confidential information can take various forms and be held and transmitted in a variety of ways, for example:

- manual records (files);
- computerised records and memory sticks;
- written reports/minutes/agendas/file notes etc;
- letters, memos, messages;
- telephone calls;
- face-to-face;
- Email;
- Intranet/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 Headteacher or line manager.

Responsibility of individuals in possession of sensitive information

As a general rule, 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.

The nature of the information:

- how sensitive is the information?
- how did it come to your attention?

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?

The most appropriate method of communication:

- verbal;
- written;
- Email;
- in person.

The potential consequences of inappropriate communication.

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

Particular Responsibilities

- Sensitive information should be kept secure.
- Filing cabinets should be kept locked when unattended.
- Child protection information is kept in a separate, secure filing cabinet or/and on CPOMS.
- 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 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 recipient's name and position.
- If it is necessary to supply personal files through the external mail, this must be effected 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 by shredding it.
- Personal data should not be used for training or demonstration purposes where fictional data can be used.

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

- Machines must be locked when unattended.
- Machines should be switched off over night.

Computer files should be kept securely.

- Passwords should be used and these must not be disclosed to colleagues 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 on the school server.
- Any confidential information held on a memory stick must be encrypted or password protected.

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 post within the school.

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 will have a direct interest in education and schools and even the closest of 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.

- Line Managers 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 line managers and those responsible for writing references. Exceptions may apply in the case of legal proceedings.

Employee's should use their discretion in these matters and if in doubt, should seek advice from their Headteacher.

Child Protection

Professional confidentiality

Confidentiality is an issue which needs to be discussed and fully understood by all those working with children, particularly in the context of child protection. A member of staff must never guarantee confidentiality to anyone about a safeguarding concern (including parents / carers or pupils), or promise to keep a secret. In accordance with statutory requirements, where there is a child protection concern, this must be reported to the designated safeguarding lead and may require further referral to and subsequent investigation by appropriate authorities.

Information on individual child protection cases may be shared by the designated lead (or deputy) with other relevant staff members. This will be on a 'need to know' basis only and where it is in the child's best interests to do so.

Records and information sharing

Well-kept records are essential to good child protection practice. Our school is clear about the need to record any concern held about a child or children within our school and when these records should be shared with other agencies.

Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can reduce the risk of harm. Whilst the Data Protection Act 2018 places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing information where there are real safeguarding concerns. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Generic data flows related to child protection are recorded in our Records of Processing Activity and regularly reviewed; and our online school privacy notices accurately reflect our use of data for child protection purposes.

Any member of staff receiving a disclosure of abuse or noticing signs or indicators of abuse, will record it as soon as possible, noting what was said or seen (if appropriate,

using a body map to record), giving the date, time and location. All records will be dated and signed and will include the action taken. This is then presented to the designated safeguarding lead (or deputy), who will decide on appropriate action and record this accordingly.

Any records related to child protection are kept in an individual child protection file for that child (which is separate to the pupil file). All child protection records are stored securely and confidentially and will be retained for 25 years after the pupil's date of birth, or until they transfer to another school / educational setting.

Where a pupil transfers from our school to another school / educational setting (including colleges), their child protection records will be forwarded to the new educational setting. These will be marked 'Confidential' and for the attention of the receiving school's designated safeguarding lead, with a return address on the envelope so it can be returned to us if it goes astray. We will obtain evidence that the paperwork has been received by the new school and then destroy any copies held in our school. Where appropriate, the designated safeguarding lead may also make contact with the new educational setting in advance of the child's move there, to enable planning so appropriate support is in place when the child arrives.

Where a pupil joins our school, we will request child protection records from the previous educational establishment (if none are received).

The Consequences of revealing confidential information without authority

Staff should ensure that they are familiar with the 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 and other line managers 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, which could result in dismissal.

The implementation of this Policy is the responsibility of all members of staff. It has been agreed by the governing body in the summer term 2023.

Signed by the Chair of Governors:

Date:

To be reviewed: Summer Term 2025