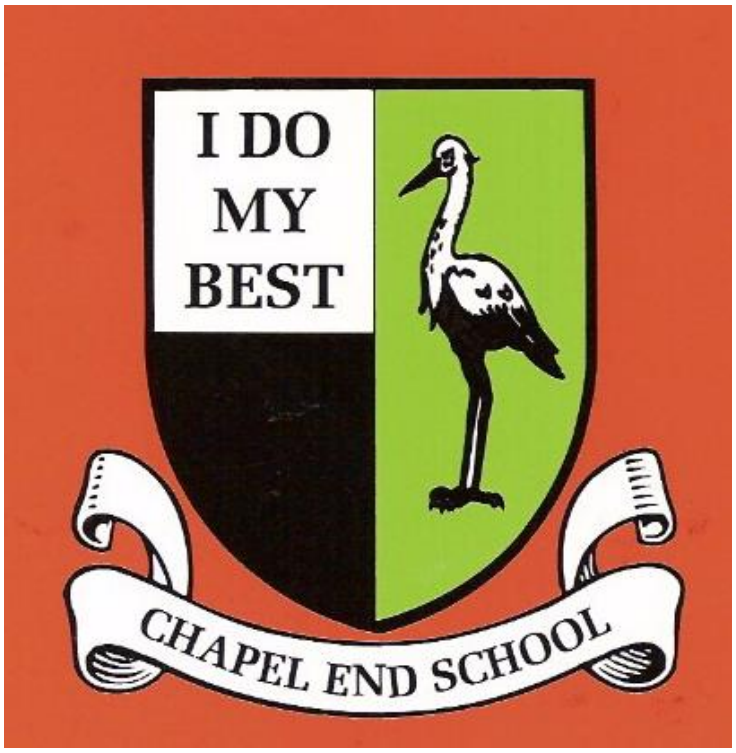

Chapel End Primary School and Nursery GDPR policy

'Mission Statement.'

We aim to provide our children with the highest possible standard of education, through quality teaching and learning, in a happy caring environment.

We will do the best WE can to enable our children to do the best THEY can.

This policy was approved by:	Full Governors
Date	Autumn 2022-2023
Review Date	Autumn 2024-2025

Introduction

This policy outlines how Chapel End Primary School delivers an effective approach to ensuring compliance with the Data Protection Act 1998.

The Data Protection Act 1998 places a legal obligation on all organisations to process personal data in accordance with eight Data Protection Principles set out in the Act.

The legislation requires Chapel End Primary school to:

Put in place an appropriate Policy;
Allocate responsibility within the organisation;
Ensure issues are communicated throughout the organisation.

Personal data is data which relates to a living individual and which allows the relevant individual to be identified either on its own or when it is combined with other personal data held.

Chapel End will gather and process personal information about staff and clients in order to operate effectively.

The School, acting as the custodians of personal data, recognise the legal and moral duty to ensure that personal data is handled properly and confidentially at all times.

Policy Statement

This Policy document outlines how Chapel End Primary School delivers an effective approach to ensuring compliance with the Data Protection Act 1998.

The aim of this policy is to ensure that personal information is:

Fairly and lawfully processed
Processed for specific purposes
Accurate, relevant and not excessive
Kept accurate and up to date
Not kept for longer than necessary
Processed in line with the data subjects (individuals) rights
Kept secure
Not transferred to other countries without adequate protection

Scope

This policy applies to all personal data held both on paper and by electronic means.

This policy covers the whole lifecycle of personal data including:

The obtaining of data;
The storage and security of the data;
The use and disclosure of the data;
The sharing of data;
The disposal and destruction of the data.

This Policy applies to all Employees and third parties working for or on behalf of the school who have access to school information in any format, network and systems. For the purpose of this policy the term 'Employee' refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

This policy should be read in conjunction with the Data Protection Code of Practice.

data_sharing_code_of_practice.pdf (ico.org.uk)

Data Protection Act 1998

Data Protection Principles

Chapel End will maintain appropriate safeguards to ensure adherence to the eight Data Protection Principles of the 1998 Act, These Principles should be adhered to at all times:

1. The collection and use of personal data will be done in such a way that recognises the Fair Processing Code, i.e. that personal data are obtained fairly and lawfully. As such the data subject should be notified of any processing by issuing a Fair Processing Notice. Particular consideration should be given to the processing of sensitive personal data, including payment card data. Parents are informed of this process during their child's induction.
2. Personal data will only be obtained and processed for the purposes specified in the notification and in pursuit of the school's business objectives, and should not be processed in any manner incompatible with that purpose (or those purposes).
3. Personal data will be collected and processed on a 'need to know' basis, ensuring that it is fit for the purpose and not excessive.
4. Steps will be taken to maintain the accuracy and currency of data. Staff training and procedural updates will ensure this.
5. Personal data will not be kept for longer than is necessary and will be disposed of at a time appropriate to the purpose for which it was collected. Paper data will be disposed of professionally. Electronic data will be deleted through the IT Service Provider.

6. The rights of individuals to whom personal data relate will be respected and steps taken to ensure that these rights may be exercised in accordance with the Act.
7. Appropriate security measures will be taken, both technically and organisationally, to protect personal data against damage, loss or abuse. All electronic systems are backed up daily in case of a disaster. Staff are required to save all information to the school's network.
8. The movement of personal data will be done in a lawful way, both inside and outside the organisation, with suitable safeguards in place at all times. Staff require permission from the headteacher to take personal data off site for meetings.

Data Subjects

The rights of individuals (data subjects) should also be observed and Chapel End Primary will ensure that these rights can be fully exercised under the Data Protection Act. These include:

The right to be informed that processing is taking place;
The right of access to their own personal data;
The right to prevent processing in certain circumstances;
The right to correct, rectify, block or erase information which is regarded as wrong information.

Information Commissioner's Office

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Commissioner is an independent authority reporting directly to UK Parliament.

Under the Data Protection Act, the Council is required to maintain an up to date and accurate 'Notification' with the ICO. Chapel End updates this annually.

The school will inform the ICO of any serious data breaches.

Responsibilities

Data Protection Officer

The Data Protection Officer is a member of senior management who has overall responsibility for Data Protection in the school. This is the Headteacher, Mr Hewitt.

The Data Protection Officer for the school is responsible for gathering and disseminating information and issues relating to Data Protection.

The Data Protection Officer is responsible for ensuring that the Council's Notification to the ICO is accurate and maintained up to date.

The Data Protection Officer is also the key contact with the ICO.

Employees

All Employees will be responsible for safeguarding the personal data in their care. This carries with it a responsibility to abide by this Policy, the Data Protection Code of Practice, and related policies, procedures and legislation. Staff training and following all policies, procedures and guidance will make this policy effective.

Review and Governance

This policy will be subject to an annual review by governors of the school, and where changes in legislation require, more frequent.

Policy Compliance

Breaches of this policy will be investigated under the school's Disciplinary Policy and Procedures for all employees.

Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

Under the Data Protection Act 1998 legal liability for the safeguarding of personal data falls both to the organisation and individually to its employees. Prosecutions can be undertaken under the Data Protection Act.

Code of Practice

The purpose of this Code of Practice (Code) is to ensure that the standards which the school wishes to adopt are communicated in a way that ensures compliance with the Act in all activities which involve the handling of personal data. It is designed for use by all employees and should be consulted for guidance on operational matters in relation to Data Protection.

This Code should be read in conjunction with the Data Protection Policy, which sets out the key commitments in relation to Data Protection. The Code details how the Policy should be put into practice.

Definitions of the terms used

Personal data

Personal Data is data which relates to a living individual (including any expression of opinion about the individual) who can be identified from the data, or from the data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

Sensitive Personal Data

The Act designates certain types of personal data as sensitive and requires that more stringent standards and safeguards are applied to the processing of it. The categories of data which the Act specifies as sensitive are as follows:

Racial or ethnic origin;
Political opinions;
Religious beliefs or other beliefs of a similar nature;
Trade union membership;
Physical or mental health or condition;
Sexual life;
The commission or alleged commission by the data subject of any offence;
Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Other types of data, such as financial details, which are not designated “sensitive” and protected as such by the legislation, should nonetheless be treated with sensitivity.

Data Controller

The Data Controller is described as determining the purposes for which and the manner in which personal data are processed. This may be an individual or an organisation. The processing may be carried out jointly or in common with other persons.

Data Processor

The Data Processor is a person who processes personal information on the Data Controllers behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

Notification

Notification is the process by which a Data Controller’s processing details are added to a register. Under the DPA 1998, every Data Controller who is processing personal information needs to notify, unless they are exempt. Failure to notify is a criminal offence. Even if a Data Controller is exempt from notification, they must still comply with the Data Protection principles.

The Information Commissioners Office (ICO) maintains a public register of Data Controllers.

The Data Protection Principles

The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything you do with personal data, except where you are entitled to an exemption.

So the key to complying with the Act is to follow the eight data protection principles.

Principle 1 – Fair and Lawful

Personal data shall be processed fairly and lawfully.

The school collects data for many different purposes in connection with the provision of services. Whenever personal data is collected from an individual, we will consider the following issues.

What is Processing

"Processing" broadly means collecting, using, disclosing, retaining or disposing of personal data and if any aspect of this is unfair (fairness generally requires you to be clear and open with individuals), there will be a breach of the first data protection principle.

In practice, this means:

- Personal data must only be collected for specific purposes which are in accordance with the law and our legitimate business objectives.
- Individuals should be supplied with appropriate **privacy notices** when collecting their personal data.
- All processing which is undertaken in the Council must be covered in our Notification to the ICO.
- Individuals must be informed about why we are collecting their data and what we intend to do with it (unless this is obvious), including who we will disclose it to.
- Handle individual's personal data only in ways they would reasonably expect.
- Not using their information in ways that unjustifiably have a negative effect on them.

Processing for additional purposes

Data can only be processed for specified purposes, and should not be processed in any manner incompatible with that purpose (or those purposes). Additional processing, which must in any case be in accordance with legal constraints and the Council's legitimate interests, is only permissible under the following circumstances:

- The explicit consent of the data subject has been obtained;
- The processing is for one of the exempt purposes detailed in Part IV (Exemptions) of the Data Protection Act 1998.

What is Lawful?

"Lawful" refers to statute and to common law, whether criminal or civil. An unlawful act may be committed by a public or private-sector organisation.

Privacy/Fair Processing Notice

Data subjects must be informed about why their information is being collected, what it will be used for and who it will be disclosed to. Data subjects must not be deceived or misled as to the purpose or purposes for which their personal data are to be processed.

This is done through a written statement usually provided near the declaration section (if appropriate) on data collection forms, although the information must also be provided even if the data is collected from individuals in any other way. This is distributed during induction days at Chapel End Primary.

Principle 2 – Purposes

> Personal data shall be obtained only for one or more specified and lawful purposes, and *shall not be further processed in any manner incompatible with that purpose or those purposes.*

At Chapel End Primary we are open about the reasons for obtaining personal data. What we do with the information is in line with the reasonable expectations of the individuals concerned.

In practice, this means that we will:

- Determine the purpose or purposes for which data is to be used before the data is collected.
- Be clear from the outset about why you are collecting personal data and what you intend to do with it.
- Comply with the Act's fair processing requirements.
- Ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Principle 3 – Adequacy

> *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*

In practice, it means you should ensure that:

- We hold personal data about an individual that is sufficient for the purpose you are holding it for, in relation to that individual. For instance it would never be necessary to collect details of a person's political affiliation on a Council Tax form.
- We do not hold more information than you need for that purpose.

We should identify the minimum amount of personal data you need to properly fulfil your purpose. We should hold that much information, but no more.

Consideration must be given to data requirements in relation to distinct groups of individuals. For instance in the case of electoral registration date of birth data is collected only from rising 18s as the Electoral Registration Officer needs to be aware of those individuals who are approaching voting age. This detail is not, however, collected from any other age group.

Where personal data is collected we should ensure that reviews of collection processes and procedures are undertaken on at least an annual basis..

Reviews of data collection should check the following:

That the purpose for which data is collected continues to be lawful and appropriate;
That the data collected is no more than is needed for the purpose(s);
That Chapel End Primary' Notification and the information given to data subjects continue to reflect actual processing and are amended where necessary;
That checks are made to ensure the accuracy of collected data.

Principle 4 – Accuracy

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

It is the responsibility of those who collect personal data to ensure that the data is accurate and up to date.

To comply with these provisions we will:

Take reasonable steps to ensure the accuracy of any personal data you obtain.
Ensure that the source of any personal data is clear.
Carefully consider any challenges to the accuracy of information.
Consider whether it is necessary to update the information.

We will ensure that adequate verification is undertaken so that the risk of damage or distress being caused unnecessarily to the data subject is minimised. An appropriate method should be chosen according to the nature of the data collected. The following could be used:

Check details with data subjects (this could be done on an annual basis).
Run internal logic checks on information you receive to see if it is consistent with other information you already hold.
Take the opportunity to check details if the data subject calls you.

Principle 5 – Retention

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, it means that we will:

Review the length of time you keep personal data.
Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it.
Securely delete information that is no longer needed for this purpose or these purposes.
Update, archive or securely delete information if it goes out of date.

To meet this condition the Council has a Retention Schedule in place (see Section 5) and all personal data should be disposed of, or retained in accordance with the Information & Records Management Policy.

Personal/confidential information must always be disposed of as confidential waste.

Principle 6 – Rights

Personal data shall be processed in accordance with the rights of data subjects under this Act.

We must ensure that individuals are able to exercise the rights which the Act gives them.

The rights of individuals that it refers to are

To access to a copy of the information comprising their personal data;
To have inaccuracies in data corrected;
To prevent the use of their personal data for direct marketing purposes;
To prevent the use of their data for purposes which would cause them undue damage or distress. The Data Subject has a right to send a notice to the Data Controller requiring him to stop the processing. This is called a 'Data Subject Notice'.
To require that no decision which significantly affects that individual is based solely on the processing by automatic means of their personal data. The individual can require a Data Controller to provide them with an explanation of how a particular decision has been made and to request that any decision made solely by automated means be re-evaluated manually.
To claim compensation through the courts from a Data Controller for damage, and in some cases distress, caused by a breach of the Act.
To ask the ICO to investigate and assess whether the Data Controller has breached the Act.

The school must respond to a written request from a Data Subject relating to any of their rights under Section 7 of The Act. For further clarification on the rights of the Data Subject you may contact the SIMO

Principle 7 – Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The school must take adequate steps (both technical and organisational) to ensure that personal data is secure. This applies to both manual data and data held electronically.

Security of data must be considered and appropriate measures applied through all the stages in processing from collection through to use and disposal.

Data processing includes all operations from collection through to disposal. Security provision at every point of processing must be considered.

Care must be taken to judge what security is necessary and appropriate by assessing the risks involved in any business process. The greater the potential harm, the tighter the security must be. By definition, breach to information which could lead to financial loss or physical or mental damage or distress is particularly sensitive in this context.

Security of data held in manual systems

The physical security both of the files themselves and of the locations where they are stored has been considered:

The risks to physical security must be assessed in all cases.
Lockable cupboards, filing cabinets and offices have been provided where necessary and procedures put in place to ensure access to secure files is controlled. Staff must seek permission from headteacher to remove any personal data from the premises.
Personal data must always be filed away in a lockable place.
A clear desk policy should be in operation.
Unauthorised access must be prevented.
Archived data is stored safely.
Archive data sets are labelled so that they are readily accessible.

Security of data held in computerised systems

This is covered under the Computer Security Guidance as part of the Computing Policy.

The organisation of office accommodation to protect data

The organisation of office accommodation has been assessed in the following terms and appropriate action taken to ensure security:

The positioning of workstations
The means of access to the office and to files and computer systems in the office is through a keycode.
Lockable storage is provided
The privacy of phone conversations has been managed
The security of premises when not in use will be locked
The clear desk policy should be in operation.

Principle 8 – International

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 protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Restrictions on Data Transfer Outside of the EEA

There are provisions in the Act to protect personal data from abuses beyond our national borders. The UK's Data Protection legislation is based on a European Union Directive which has been written into the laws of all countries within the EEA

In countries outside the EEA personal data may not be protected. For this reason one of the provisions of the legislation is that personal data must not be transferred outside the European Economic Area to countries without adequate protection unless the data falls under the exemptions laid out in the Act.

This restriction applies to countries outside the EEA which do not have adequate legal safeguards in relation to personal information. This includes the USA. For more details, please contact the SIMO.

The activities of the Council will not usually necessitate the transmission of personal data to destinations outside the UK. However, with the rise of 'Cloud' services (e.g. Dropbox, Google Drive etc.) due consideration must be given both to the legal safeguards which exist in the destination country and to ensuring the security of the data on its journey to that destination. For more details, please contact Business IT.

Publication on the Internet

The main implication for the school of the restriction on overseas transfer is in relation to the Internet.

Access to information on the Internet cannot be controlled and any data posted on a website can be seen by Internet users in any country. In effect, to publish personal data on the internet in a work related capacity is to transfer it overseas to all countries outside the EEA.

For this reason personal data must never be published on the Internet without the explicit consent of the Data Subject. Chapel End Primary actively seeks permission for this.

Dealing with requests for disclosure

The school may receive requests for personal data, including requests from other Council Departments, elected Members and other organisations.

The legislation is clear that personal information must be treated as confidential and not disclosed to those who do not have a legitimate right to have it.

All requests must be recorded along with the date of the request, the decision made on whether to release the information, the basis for this and the date of the decision.

Evaluating a request for the disclosure of information

Careful consideration must be given to the requirements of the legislation and caution should always be taken in our approach to any requests for disclosure.

The Headteacher can advise in any case where there is uncertainty but any queries should be referred initially to the Office Manager or other member of the SLT.

Requests for disclosure from Council records should only be accepted when made in writing. They should be on the official letterhead of the requesting organisation or from a legitimate email address. If you have any doubt about the email address please contact the headteacher.

On some occasions, organisations such as the Police, may request information quoting Section 29 of the Act[1]. The request, together with any information that is disclosed, must be recorded.

[1] Section 29 of the Data Protection Act allows the disclosure of information for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or of any imposition of a similar nature. An organisation is not compelled to disclose the information, but the Act allows them to if they believe that the reason is justified.

All requests for personal information should include the following:

- Details of what information is required (this should be as detailed as possible)
- Reason(s) why the information is needed
- Details of any legal justification for the request including the title of the relevant legislation, the section/paragraph numbers **and** the relevant text.

Where it is agreed that a disclosure should be made it must be stipulated to the party requesting the information that the data is disclosed solely for the purposes of the specific enquiry concerned. It must not be used for any further purpose or disclosed to any other party without consent.

Disclosure of information to elected Members

The information which may be disclosed to the Council's elected Members is dependent upon which role they are fulfilling when making a request for data. They will act in one of the following capacities:

- As a member of the Council, for instance as a member of a Committee;
- As a representative of residents of his or her ward, for instance in pursuing complaints;
- As a representative of a political party, particularly at election time.

All disclosure requests, reasons for disclosing or not, and details of what information is disclosed, must be recorded together with dates and any other information relevant to the case.

Retention scheduling and disposal of data

Under the Act organisations must ensure that personal information is not kept for longer than is necessary to fulfil the purpose(s) for which it has been collected, and that it is disposed of in a timely manner.

Retention Scheduling

The public and stakeholders alike will expect that their interests are being safeguarded, and the accurate retention will assist in meet their expectations.

To ensure that data is disposed of when no longer needed we will use the guidance from the Local Government Classification Scheme.

The objectives of this schedule are:

- Assist in identifying records that may be worth preserving permanently as part of local authority guidelines.
- Prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial or other requirements of public administration.
- Promote records management practices.

The rationale for this document has been based upon guidelines published by the Records Management Society (Retention Guidelines for Local Authorities), or where appropriate, the rationale is based upon local business needs.

We will follow all legal requirements for the retention of documentation.

It is also the responsibility of each area to make sure that appropriate staff are kept informed of the current retention period for documents or records that they are accountable for.

Some key documents and documents of either historic interest or intrinsic value should be kept permanently.

Maintaining the Retention Schedule

A systematic approach is taken annually to the management of filing systems (electronic or paper) to ensure that any schedule for retention and destruction operates effectively through:

- Regular housekeeping being carried out on all records to ensure compliance with the Retention Schedule.
- Where paper records are retained in storage, a record should he held of their location, date for destruction and actual destruction date.
- Staff ensuring that retention periods specified in the Retention Schedule are complied with.
- Where a decision is taken to retain documents beyond the specified retention period, the reason should be recorded and approval obtained from senior management.
- Responsible Officers investigating whether data held on stand-alone databases can be deleted in accordance with specified retention dates.

Disposal of Data

It is important to keep in mind that in the course of the schools' everyday business many documents are generated that serve no purpose after relatively short periods of time. Many documents will relate to completed matters where, realistically, the risk of subsequent litigation or other dispute is minimal, if not non-existent. Long-term retention of such documents is counterproductive.

Personal data which is ready for disposal should always be treated as confidential waste and must be kept secure at all times. It should be disposed of in accordance with the formal Retention Schedule, and one of the following methods should be used.

- Shredding in-house: For small quantities of confidential waste, each Employee can shred their own documents as and when it is identified, and dispose of it in an office re-cycling container.
- The corporate system for the disposal of confidential waste: Large/Medium quantities of confidential waste may be disposed of by placing in sacks/bags clearly marked as 'Confidential Waste' and contacting Environmental Protection. Whilst this waste is awaiting collection, it is each Employee's responsibility to ensure that it remains secure. Bags of confidential waste should not be left in areas where unauthorised staff/members of the public may be able to access them.

Confidential waste is quantities of waste paper or other documentation that contains:

- Personal data, from which you would be able to identify a living individual e.g. documents which reveal the contact details or any financial details of any named living person, (unless prior permission has been given to publicise the details).

Data of a commercially sensitive nature (e.g. plans, figures, contracts, tenders, legal documents, purchasing, documents that may breach copy right etc.).

Examples of potential confidential waste are:

An unwanted e-mail that you had printed out.
A photocopy of a parents letter.
Original documents detailing planning of lessons with children's names on.
A scribbled telephone message which includes name & telephone number or email address.
This list is not exhaustive.

Rights of Data Subjects

Section 7 (along with Principle 6) of the Act defines the rights which individuals have over their personal data held by organisations.

The school must ensure that individuals whose data it holds (whether this is on paper, electronic, email etc.) are able to exercise their rights fully.

The right of Access

Individuals have the right to access information that is held about them. This is known as a Subject Access Request (SAR). All requests for information **must** be in writing. The Council cannot respond to a request made over the phone.

Any request from an individual for data that is held about them is classed as a Subject Access Request. This applies to whether the application has been made to the Council as a whole or to an individual Department.

A valid SAR should include:

the applicants full name and address
details of the specific information that the requestor requires (although a request for 'all' the data that is held is also valid)
Proof of identity or authority to disclose (if appropriate)

For further information please see the Council's Subject Access Request Procedure.

Notification

Under the Act the Council is required to maintain an up to date and accurate Notification with the ICO.

What is a Notification?

The ICO maintains a public register of Data Controllers. Notification is the name given to this registration of an organisation with the Data Protection regulator (ICO) in respect of personal data that they are processing.

Under the Act, every Data Controller who is processing personal information needs to notify, unless they are exempt. Failure to notify is a criminal offence.

The Notification must reflect all the processing which is being undertaken including processing that is done on an organisation's behalf by any third party organisations.

Keeping the notification up to date

The Office Manager is responsible for keeping the school's Notification up to date with the ICO.

The Notification should reflect the actual processing which is taking place at any given time.

Sometimes changes are made either to the type of data being processed, or to the purposes for which it is processed, or to the people and organisations it is disclosed to.

If we make any changes in processing these should always be reported to the Office Manager so that the Notification can be amended to include them.

Closed Circuit Television

The school does not use this resource.

Sending personal data

1.1 Everyone who handles personal and/or sensitive information has a duty to ensure that it is kept safe and secure and shared only with those who have a legitimate reason to see it. When information is in transit it is at risk of loss, damage, theft and inappropriate or accidental disclosure.

1.2 If it's absolutely necessary to send personal data to someone outside of the Councils Network then there are a number of things that we will consider.

Who are you sending the data to?
Have you checked them out? Are they who they say they are?
Why do they want the data?
Are you legally obliged to disclose/share this data with them?
Are they entitled to have the data disclosed to them?
Can the data be anonymised?
How do you intend to send the data?

Remember, if you disclose or share personal data to a third party before checking that you can legally do so, you may be in breach of the Act.

Even if you're legally entitled to disclose/share personal data to a third party, it must be done so securely. If it is not processed securely, again you may be in breach of the Act, and may be subject to disciplinary procedures.

Where the school receives information from third parties, it has an implied duty of care to advise them if they are in breach of legislation (such as Data Protection) with a view to ensuring that our clients can trust any partner working arrangements that are in place.

If you are sending personal data to an external organisation you should use the following guidance:

Email

When a standard email is sent between different organisations it is transmitted over the Internet. This means that the contents of the email are not particularly safe.

Email can be intercepted or misdirected, either by accident or for criminal purposes.

Where information leaves the school, it must comply with the requirements of The Act as well as the practicalities and requirements of the recipient. This includes the need to ensure that electronic records are encrypted, where necessary, and that the authorised recipient can decrypt and read them.

You must ensure that you are legally allowed to release the details of the data **before** you disclose it.

PGP Email Encryption

PGP Email Encryption will be used for sensitive personal data such as occupational reports for employees..

To use PGP you must ensure the Subject field contains *Confidential (this can be selected via Display > Additional Mail Options).

If you are having issues using TLS or PGP please contact the IT Service Desk on ext. 6525 or alternatively you can log a job through the IT Service Desk Portal.

Post

Alternatively, if you are unable to use secure email and where such information needs to be communicated and confidentiality cannot be assured, it should be sent in hard copy through the post system, via recorded delivery and be clearly marked as ‘Private and Confidential’.

Fax

The use of fax should be strictly limited to where there is absolutely no other option and only with the agreement of the recipient before the fax is sent.

If an Employee is sending a fax then they should confirm the fax number of the recipient and make sure that the recipient is waiting by the fax machine for the fax to arrive. They should also ensure that a fax receipt is received for the correct fax number, and ask for verbal confirmation that the fax has been received. Equally, if an Employee is expecting to receive a fax containing personal data, then they should make sure that they are available to collect it from the fax machine.

Collection and storage of personal data on email

Employees should be aware that personal data stored on email is subject to the provisions of the Act in the same way as data stored in any other way. The following should be noted:

Personal data on email must be collected and processed in a fair and lawful way

Personal references to customers and clients in emails should be avoided where possible.

Contracts Procedure Rules

The school has adopted the Councils contract procedure rules and will follow this policy.

Partnership working

The school works in partnership with other agencies in connection with the provision various services such as network schools.

Any personal data which is shared for the purposes of partnership working, for which the school is responsible, must be handled in accordance with legal requirements.

Information Sharing Agreements

Chapel End Primary is a partner of St. Helens Council and as such has adopted a Corporate Standard information sharing framework, which is nationally recognised. This is called the 'Information Sharing Toolkit' and provides a standardised agreement which should be used whenever setting up any sharing of information.

An agreement should:

- Help to justify data sharing and to demonstrate that the relevant compliance issues have been considered and documented.
- Explain why the data sharing initiative is necessary, the specific aims and benefits it will bring to individuals or to society more widely. This should be documented in precise terms so that all parties are absolutely clear as to the purposes for which data may be shared and shared data may be used;
- Identify clearly all the organisations that will be involved in the data sharing and should include contact details for their key members of staff.
- Contain procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing.
- Explain the types of data that are intended to be shared. This may need to be quite detailed, in some cases it will be appropriate to share certain details held in a file about someone, but not other, more sensitive, material.
- Where necessary attach 'permissions' to certain data items, so that only certain members of staff, for example ones that have received appropriate training, are allowed to access them.
- Explain the basis for sharing data clearly. Even if it is not under any legal requirement to share data the agreement should still explain how the disclosures will be consistent with the Act
- Address issues surrounding the withholding or retraction of consent.

General Information sharing principles

The processing of information must be done in accordance with appropriate legislation, including the Human Rights Act, the Data Protection Act and the Common Law Duty of Confidence which each protect the individual's right to privacy.

The ICO would expect a data sharing agreement to address the issues including:

- No secondary use by the partnership or receiving agency of disclosed data is permitted.
- When data is disclosed it must be restricted to what is sufficient to answer the stated specific query to prevent irrelevant or excessive information being disclosed.
- Data being kept accurate and up to date.
- Disclosed data not being kept longer than is necessary by the partnership or receiving agency.
- Arrangements being in place so that individual data subjects may exercise their rights under the Act.
- All stages within the information sharing arrangement having adequate technical and organisational security measures in place to safeguard the personal information, including the transmission of the data and procedures for dealing with any breach of the agreement.
- Using compatible datasets and recording data in the same way. The agreement could include examples showing how particular data items – for example dates of birth – should be recorded.
- Procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

Furthermore, each request for disclosure under a partnership arrangement must be justified by the requestor and be both lawful and in accordance with the agreed protocol.

Any requests for disclosure must be considered on a case by case basis, and care must be taken where aggregated data is shared so that individuals cannot be identified.

Sources of further information, advice and guidance

The Intranet

The Councils Intranet contains information and advice in respect of all aspects of Information Management, including Data Protection.

Data Protection on St. Helens Council Website

Information about Data Protection is included on the Councils website. It provides details to members of the public in relation to their rights under the Act, including how to find out what information the Council may hold about them (Subject Access Request).

System & Information Management Officer

The SIMO (in consultation with the Data Protection Officer) is responsible for communicating Data Protection issues throughout the Council and does this in a number of ways:

- Produces information and guidance on Data Protection issues for the Council;
- Maintains the Data Protection information on the Council's intranet;
- Distributes information through the Departmental Information Representatives;

Communicates information direct to staff as appropriate.

Any queries relating to Data Protection should be directed to:

Andy Paton, Ext: 3474, Email: andrewpaton@sthelens.gov.uk

The Information Management Group

The Information Management Group (IMG), which brings together the Departmental Information Representatives, acts as a hub for the communication of Data Protection issues to Departments.

Briefing Structure

The briefing structure in each Department provides a further means for the dissemination of information from central sources (IMG or the SIMO).

Information Commissioners Office (ICO)

The Information Commissioner is the Regulator for Data Protection in the UK.

The Commissioner has a website containing information and official guidance on Data Protection issues. Access to the Register of Data Controllers is also available from here.

The site can be found at: https://ico.org.uk/

The Commissioner's Office may also be contacted direct with queries about the UK's Data Protection regime:

Office of the Information Commissioner

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

Helpline: 01625 545745