Defford and Besford Church of England
Primary School

"Through Faith, Friendship and Fun we Learn and Grow"

Data Protection Policy

Ratified by Governing Body : January 2025
Review date : January 2027

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 4
5. Roles and responsibilities 5
6. Data protection principles 5
7. Collecting personal data 6
8. Sharing personal data 7
9. Subject access requests and other rights of individuals 7
10. Parental requests to see the educational record 9
11. Photographs and videos 9
12 Data protection by design and default 10
13. Data security and storage of records 10
14. Disposal of records 11
15. Personal data breaches 11
16. Training 11
17. Monitoring arrangements 11
18. Links with other policies 12
Appendix 1: Personal data breach procedure 13

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Date of birth • Home address • Email address (such as name.surname@company.com) • Identification number • Location data • Online identifier, such as a username or Internet Protocol (IP) Address It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin

	• Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **Mr James Weaver** and is contactable via the school office, **01386 750321.**

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner

- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO. An education record request is dealt with in section 10.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters (1 capital), numbers and at least 1 special character are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment policy on acceptable use
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable use policy
- Safeguarding including child protection
- E safety policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify headteacher. The headteacher will work with the staff member, using the Incident reporting form (Appendix 3) to consider the nature of the breach. The headteacher will then determine the appropriate next steps, this is likely to involve sharing the form with the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered without permission
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system. The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*

- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Appendix 2: Tips to protect data

Information on paper

- Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.
- Confidential documents must not be left on display or unsupervised.
- Store confidential information in locked cabinets, returning them to these cabinets when not required.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.
- Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.
- Spoiled photocopies and prints may still be confidential. Do not put them straight into the wastepaper bin, dispose of them as confidential waste. Always check that originals have been removed from the device as well as copies.
- Dispose of confidential paper by shredding or put in a confidential waste bag and follow confidential waste disposal procedure. Do not dispose of confidential waste in a wastepaper bin or anywhere else.
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

Electronic information

- All confidential information must be stored on Defford-cum-Besford C.E. First School approved electronic devices or systems with access controlled/restricted, e.g. the Defford-cum-Besford C.E. First School network or the school's password protected Drive on Microsoft OneDrive.
- Confidential information must not be stored on local unencrypted hard drives.
- If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by Defford-cum-Besford C.E. First School
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g. through windows or while waiting in public areas.
- Notebook PCs, handhelds or any other portable ICT device must not be left unattended in any public area (see Mobile Computing below).
- Individual user id/passwords must not be shared with anyone, including other staff members and governors, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the Defford-cum-Besford C.E. First School network using your network id.
- Passwords must not be written down and left with any equipment or accessible by anyone else.
- Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already.
- Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.
- If you find you have access to confidential information that you believe should be restricted, you should notify the Headteacher and the Chief Protection Officer immediately. They will then notify the Worcestershire Legal Services (our DPO service).

Information via the post

- Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeon holes'.
- Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.
- If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'. A return address must be shown on the envelope and you should consider double bagging the package.
- Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address.
- When using a mailshot or multiple mailings, have a procedure in place to check you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.
- Consider using signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.
- Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.
- If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

Information via email

- Defford-cum-Besford C.E. First School does not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.
- If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.
- Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.
- If sending to a list/group of parents or others, send using 'blind copy' (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.
- Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;
    - you are using an encrypted email service provided by Defford-cum-Besford C.E. First School, or
    - the information is encrypted / password protected in an attachment, or

    - you are sending to an approved Defford-cum-Besford C.E. First School email address, e.g. a school email address
    - you are sending to an e-mail address which utilises the same server – for schools which use the Worcestershire e-mail system this includes all other schools with this system as well as Worcestershire County Council.
- Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the GDPR. If a permanent record is required they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as Defford-cum-Besford C.E. First School records.
- Defford-cum-Besford C.E. First School Confidential email must not be forwarded to your own personal email account for private use.

Information via telephone calls

- Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.

Information via conversations

- Staff should remember that even though they may be on Defford-cum-Besford C.E. First School premises there may be pupils and visitors around.
- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the proximity of others who may be able to hear in public places.

Appendix 3

Personal Data Security Breach – Incident Reporting Form

This form should be used to provide information to the Data Protection Officer when there has been a serious breach and consideration needs to be given to whether the breach should be reported to the ICO.

The aim of the form is to gather detailed information in order to understand the gravity of the breach, including its impact and what must be done to reduce the risk to personal data and the individuals concerned.

It is imperative that as much information as possible is provided.

The information will be used to review policies and procedures and assess whether changes
are required.

Breach log no: _____

Breach log reference: _____

1. Details of the breach

a) Date and Time of the Incident

b) Number and description of individuals whose data is affected (eg 3 year 2 pupils)

c) Department (if relevant)

d) Nature of the breach

e) Description of how breach occurred

2. Reporting

a) When the breach was reported to you?

b) How did you become aware of the breach?

3. Personal Data

a) Full description of personal data involved (without identifying individuals)

b) Have all of the affected individuals been informed of the breach?

c) If not, why?

d) Has the personal data in this incident been inappropriately processed or further disclosed?

4. Consequence of the Breach?

a) Describe the risk of harm to individuals as a result of this breach?

b) Is there a risk of identity fraud as a result of this breach?

c) Has a formal complaint been received from any of the individuals affected by the breach?

If yes, please provide details.

5. Measures taken or to be taken?

a) What immediate action was taken?

b) Has the data been retrieved? – if yes, please specify date and time. Has any further action been taken to minimise the possibility of a repeat of such an incident?

c) Has there been a breach of governance policies and procedures?

e) Have the employees involved with the incident received data protection training?

Please provide details.

f) Is further data protection training required?

Completed by:

Name: _____

Job Title: _____

Signature: _____

Date: _____