



Sheepscombe Primary School

DATA PROTECTION POLICY

This policy was adopted at a meeting of:	FGB
Held on:	4 th June 2024
Date to be reviewed	June 2025
Signed on behalf of the Governors:	
Name of signatory:	Sachi Hatakenaka
Signed by Head teacher	
Name of Headteacher	Vicky Dangerfield



Sheepscombe Primary School and Little Lambs Nursery fully recognises its responsibility for safeguarding children and the importance of raising awareness of child protection issues. We discharge our responsibility with the attitude that 'it could happen here' where safeguarding is concerned. Any actions we take will be in the best interests of the child and compliant with the relevant statutory guidance.

This policy applies to all staff and volunteers within the school.

Designated Safeguarding Lead (DSL) -Vicky Dangerfield (Headteacher)

Deputy DSL's -Caroline Powell, Richard Crocker, Rob Gardner

Safeguarding Governor - Tessa Lentel

Gloucestershire Safeguarding Children Board (GSCB) procedures

[Gloucestershire Safeguarding Children Partnership | Gloucestershire Safeguarding Children's Partnership](#)

This policy should be read in conjunction with:

Safeguarding and Child Protection Policy
[Sheepscombe Primary School - Safeguarding](#)

Code of Conduct and Whistle Blowing Policy
Managing Serial and Persistent Complaints Policy
Low level complaints against staff policy
Acceptable use
[Sheepscombe Primary School - Policies](#)



Contents Page

1. Introduction
2. Scope / Our Commitment
3. Principles of Data Protection
4. Responsibilities
5. Definitions of Data Protection
6. Legal Bases
7. Fair Processing / Privacy Notice
8. Sharing Data
9. Photographs and Videos
10. Data Protection Rights of the Individual
11. Security of Data
12. Location of Information and Data including My Concern
13. Data Disposal
14. Complaints
15. Data Breach
16. Related Policies / Documents
 - Annex A DPIA for My Concern software
 - Annex B Linking the DPIA to the General Data Protection Principles



Data Protection Policy General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

Safeguarding - the DPA 2018 and GDPR do not prevent or limit the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protection of children [Keeping children safe in education - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/consultations/keeping-children-safe-in-education) See also the school's Safeguarding policy.

1. Introduction

In order to work effectively Sheepscombe Primary School and Little Lambs Nursery, hereafter known as Sheepscombe Primary School) has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, governors, members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means. We are all responsible for its safe handling.



This document sets out the principles of data protection, our responsibilities, and the access rights of individuals, as well as information sharing and complaints

2. Scope/ Our Commitment

This policy applies to all staff, governors, contractors, agents, representatives and temporary staff, working for or on behalf of the School. The requirements of this policy are mandatory for all of these parties.

Sheepscombe Primary School regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the school and those it interacts with. The school will ensure that it treats personal information correctly in accordance with the law.

Sheepscombe Primary School fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

Sheepscombe Primary School is committed to ensuring that their staff are aware of data protection policies, legal requirements and that adequate training is provided.

Changes to data protection legislation, under the GDPR and DPA, shall be monitored and implemented in order to remain compliant with all requirements.

3. Principles of Data Protection

The GDPR outlines seven key principles for anyone who processes personal data. These principles form the basis of our approach to processing personal data.

[Guide to data protection | ICO](#)

[Key definitions of the Data Protection Act | ICO](#)

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- ensure that data is not kept for longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

4. Responsibilities

Sheepscombe Primary School is registered as a data controller with the ICO and will renew this registration as required.



Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

[Register of data controllers | ICO](#)

Data breaches shall be notified within 72 hours to the individual(s) concerned and the ICO.

The members of staff responsible for data protection within the School are mainly School Business Manager, Headteacher and SLT. However all staff must treat all pupil (or other relevant) information in a confidential manner and follow the guidelines set out in this document.

We have appointed Gloucestershire County Council as our Data Protection Officer. They can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

5. Definitions of Data

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual but need not be sensitive information. The GDPR makes a distinction between personal data and "special category" (sensitive) data. Special category personal data requires stricter conditions for processing.

Personal data is Defined in s(1) of the GDPR, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller' (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.

Special Category Data is information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.

6. Processing Personal Data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law. When special category personal data, criminal conviction data or data about offences, is processed, a lawful basis and additional condition will be satisfied.

- 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/carers when appropriate in the case of a pupil) has freely given clear **consent**

7. Fair Processing / Privacy Notice

We shall be transparent about the intended processing of all data including criminal offence data and communicate these intentions via notification to staff, parents and pupils prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

8. Sharing Data

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example local authorities, Ofsted, or the Department of Health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Any proposed change to the processing of an individual's data shall first be notified to them.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from **Sheepscombe Primary School** to another school, their records and other data that relates to their health and welfare will be forwarded on to the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.



- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information on to courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of suspected child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Education division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child's or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

9. 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, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.



Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns or third party benefactors (such as charities or companies who provide financial support to the school).
- Online on our school website or social media pages/ feeds.
- Videos and photographs may be labelled with pupil's names or tutor groups when used in this way.

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.

10. Data Protection Rights of the Individual

Data Access Requests (Subject Access Requests)

All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Sheepscombe Primary School

No charge will be applied to process the request.

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, 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)
- Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

11. Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

[Risk and impact assessments | ICO](#)

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of their competence in the security of shared data.

12. Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard in the Head teacher's office or locked cabinet or cupboard in the school office. The only exception to this is medical information that may require immediate access during the school day is stored with the School Business Manager in the first instance.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.



- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- Laptops and USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

My Concern software and Data Protection

Sheepscombe Primary School operates a cloud based system or 'hosted solution', called MyConcern. Access to MyConcern is through the internet. Resources are retrieved from MyConcern via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to MyConcern is through a web browser.

As such Sheepscombe Primary School must consider the privacy implications of such a system. The Data Protection Impact Assessment (DPIA) is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Sheepscombe Primary School recognises that using a 'hosted solution' has a number of implications. The school recognises the need to have a good overview of its data information flow. The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act.

It considers the need for a cloud based system and the impact it may have on individual privacy. The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

Sheepscombe Primary School aims to undertake a review of this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps: 1. Identify the need for a DPIA. 2. Describe the information flow. 3. Identify data protection and related risks. 4. Identify data protection solutions to reduce or eliminate the risks. 5. Sign off the outcomes of the DPIA.

The DPIA for the use of My Concern reporting software can be found in Annex A

My Concern is a software system which enables the recording and sharing of safeguarding information, including attendance concerns and behavioural information of children and families at our school.



Software components within MyConcern can extract the required information from the school's management information system SIMS and transfer it securely and in a uniform format to the desired location in MyConcern.

Please see : <https://www.myconcern.co.uk/our-privacy-policy/>

MyConcern is a hosted system which means that all updates, maintenance and management can be performed in a central location by One Team Logic Ltd (the owners of MyConcern). The platform enables Sheepscombe Primary School to improve their management of child safeguarding Information, including attendance concerns and behavioural information, held in one central location without the need for duplicate hard copy files.

The platform enables Sheepscombe Primary School to centralise the data by improving the level of granularity of data and relevant agencies.

Meetings and summaries of conversations held with relevant parties can all be recorded on the system, in a safe, secure and searchable method.

Recording sensitive pupil information electronically is password protected which will help mitigate against the risk of a data breach with the appropriate controls in place.

By opting to use My Concern the school aims to achieve the following:

1. Management of sensitive pupil information in one place
2. Security and integrity of sensitive data through a secure document vault
3. Storage of information electronically rather than manually
4. Recording information and building a chronology around the pupil
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Ability to add information from staff across the school
8. Secure access across all devices wherever the setting Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from a PC in the school.

MyConcern cannot do anything with the school's data unless they have been instructed by the school.

The school is the data controller and One Team Logic Ltd is the data processor



13. Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

[IT asset disposal for organisations | ICO](#)

The school uses Stone Computers to dispose of sensitive data that is no longer required and there is a cross shredder for the purposes of shredding confidential information on-site.

14. Complaints

Complaints about how the school processes data under the GDPR and responses to subject access requests are dealt with using the School's complaints procedure.

15. Breach of Policy

Any breach of this policy should be investigated in accordance with our Data Breach process. The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

16. Related Policies / Documentation

- Privacy Notice
- Complaints procedure
- Consent form
- CCTV
- Freedom of Information Policy



Annex A

Sheepscombe Primary School

DPIA for My Concern Safeguarding Software

DPIA screening questions and assessment

Initiative name: My Concern
Version and date: Version 1 November 2021

The following screening questions will identify if a DPIA is required. Answering 'yes' to any question will require the DPIA to be completed. You may expand on the answers as work progresses.

Number	Question	Yes /No	Comments
1	Will the initiative involve the collection of new information about individuals?	Yes	
2	Will the initiative compel individuals to provide information about themselves?	No	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? NB. This includes individuals who have previously accessed information but now work for a different organisation.	Yes	Social Care - not specific to this system.
4	Will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes	
5	Does the initiative involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No	
6	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	Yes	Social Care - not specific to this system.



7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	Yes	Safeguarding concerns
8	Will the initiative require you to contact individuals in ways which they may find intrusive i.e. invasive, indiscreet, interfering or upsetting?	No	

If all questions have been answered 'no' a copy of this document should be retained in accordance with our records retention policies and as the initiative develops reference made to the screening questions in case any answers change to 'yes'. If any question has been answered 'yes' please continue to complete the rest of this template.



Step one - Identify the need for a DPIA

Initiative outline Note - explain what the initiative aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.	My Concern will be used to collate safe guarding concerns about pupils across the school. It will also track serious incidents of misbehaviour, and concerns that parents bring to us regarding home circumstances. The system aims to ensure safe record keeping and communication of safeguarding issues. It will support the schools communication with external agencies and parents.
Why is a DPIA required? Note - this can draw on your answers to the screening questions.	The information collected is of a delicate nature, and will be the only record of the school's concerns. A loss of this data could impact on effective safeguarding of children, and a breach would affect well-being of all of the school's vulnerable families.

Step two - Describe the information flows

Information flows Note - describe how personal information is collected, stored, used and deleted explaining what information is used and what is it used for and who has access to it. It may also be useful to refer to process diagrams or another way of explaining data flows. To obtain a full understanding of information flows it is important that you consider <u>all</u> of the following information: • How many individuals will be affected?	Information is collected directly from SIMS about all 72 of our pupils and our Nursery children, and is stored on the My Concern system. The Technical Support team ensures that the integration between SIMS and MyConcern is kept constantly functioning, which enables any changes made within the MIS to be transmitted to MyConcern on a daily basis to ensure the data is accurate and up-to-date. MyConcern is hosted in Microsoft Azure data centres located in the United Kingdom. Data is not transferred outside of the EEA for any reason. This is then added to by basic and trusted users, who are all members of staff at the school, when safeguarding or behavioural incidents occur. The Designated Safeguarding Lead and the Deputy Safeguarding Leaders then have access to this information.
--	---



• How information is collected? • Why is information collected? • How will the information be stored? • For how long will the information be stored? • Where has information come from? Who will have access to the information? • How will information be deleted? • Can analysis or reporting of anonymised data sets identify an individual? • Can combining various sets of data result in the identification of an individual? • Potential risks with the information flow? • For use of existing data does the consent form/s used to collect the original data, and the associated privacy notices, cover the use of the data being considered by the initiative.	The information is kept on the live system until it is archived. MyConcern supports schools in meeting their legal obligation to hold safeguarding records until the time that the data subject reaches age 25. The information is transferred securely to the pupil's next school. This takes place by printing a chronology as a PDF or completely a direct transfer if the receiving school is also using My Concern. Anything requiring a PDF file will be delivered by hand to the Designated Safeguarding Lead at the secondary school. Some secondary schools use My Concern, which allows us to transfer the information directly within the system. The system does not allow us to delete information due to the safeguarding nature of the system. Anonymised data sets used for analysis of patterns cannot identify individuals. The potential risks are that when we pass the information onto other schools it might not arrive safely, however, transfer records include a signature sheet to reduce this possibility and the School Business Manager who is also the DDSL will always follow up with a telephone call to confirm receipt. Existing forms regarding information collection cover the type of information covered.
Advice sought and consultation Note - explain what practical steps you will take to ensure that you identify and address privacy risks. Who needs to provide advice? Who should be consulted, internally and externally? How will you obtain advice and carry out consultation?	GCC as our DPO have provided advice regarding the use of these types of system. Internally we consulted the DDSL's and the Governing body.



Step three - identify the privacy related risks

Note - identify the key privacy risks and the associated legislative compliance and corporate risks.

Annex 1 provides an extract of the GDPR principles to help you identify where there is a risk that the initiative will fail to comply with the General Data Protection Regulation or other relevant legislation, for example the Human Rights Act.

	Consequence		
Privacy risk/ issue	Identify risks to individuals	Identify legislative compliance risks	Identify associated organisation/ corporate risk
Information about more than one child involved in the incident might be stored in the same incident report.	Information related to other children could be shared with parents.	Fairness and transparency	
Errors in transferring data from one school to another.	Safeguarding information could be sent to the wrong establishment and therefore 'lost'	Accuracy	

Step four - identify privacy solutions

Step 4 - Option 1

Note - describe the action you could take to reduce risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).



You will need to score the privacy risk by multiplying the impact of the risk happening (1-3) by the likelihood of the risk happening (1-3) using the key shown in the table below. Once you have identified the solutions (mitigating actions/ opportunities) to manage or mitigate the privacy risk you need to calculate the residual score. Any privacy risk with a residual score of 6 or more should be considered high risk.

	Impact (I)	Likelihood (L)	Score (S)
1	No or slight impact	Unlikely to happen	I x L
2	Significant impact	Possible to happen	
3	Major impact	Highly likely to happen	

Ref	The Risk What can happen and how it can happen	Consequence / benefit of event happening	Inherent Risk			Mitigating Actions / Opportunities	Residual Score			Further Action Required	Risk Owner	Open/ closed
			I	L	S		I	L	S			
a)	Information related to other children could be shared with parents.	Circumstances could be exacerbated by parents finding out the details of the behaviour of other children.	2	1	2	Staff need training to ensure they do not share contents of My Concern directly with parents.	2	1	2	No	Head teacher and SBM	closed



b)	Safeguarding information could be sent to the wrong establishment and therefore 'lost'	Safeguarding information 'lost' and potentially shared inappropriately.	3	1	3	Head teacher and Deputy DSL who is the School Business Manager takes responsibility for delivering safeguarding chronologies to secondary schools either by hand or using the internal My Concern system. Egress used when necessary.	3	1	3	No	Head teacher and SBM	closed
	Data stored on My Concern is shared without consent from the individual / legal guardian and is seen as intrusive	Information for which consent has not been given is shared with agencies	3	2	6	GDPR Data Protection Act 2018 Reputation of organisation damaged. Information is used in a way that is disproportionate to need. DSL to support staff in recognising where the need outweighs the GDPR issue.	3	1	3	No	Head teacher	closed
	Incorrect information being added to the system	Potential to misinform other agencies which could have a	3	1	3	GDPR Data Protection Act 2018 Reputation of organisation damaged. Information is	3	1	3	No	Head teacher	closed



		negative impact on the individual				used in a way that is disproportionate to need. Highlight the importance of accuracy to staff using the system.							
	Data is shared with those not authorised to view	Privacy of individual is breached	2	1	2	GDPR Data Protection Act 2018 Risk to school, financial penalties required for data breach. Ensure staff that leave are deleted from system.	2	1	2	No	Head teacher	closed	



Step five – sign off and record the DPIA outcomes

Note - who has approved the privacy risks and solutions involved in this initiative? Who is responsible for implementing approved solutions?		
Risk	Approved solution	Approved by whom and date-latest check
Information related to other children could be shared with parents.	Staff training	Vicky Dangerfield September 2024 Caroline Powell
Safeguarding information could be sent to the wrong establishment and therefore 'lost'	Head teacher and SBM to manage and use of Egress when appropriate.	Vicky Dangerfield Caroline Powell September 2024
Data stored on My Concern is shared without consent from the individual / legal guardian and is seen as intrusive	DSL to support staff in recognising where the need outweighs the GDPR issue.	Vicky Dangerfield September 2024 Caroline Powell
Incorrect information being added to the system	Highlight the importance of accuracy to staff using the system.	Vicky Dangerfield September 2024 Caroline Powell
Data is shared with those not authorised to view	Passwords and security levels are set and only shared with authorised individuals. Password security is robust within school, individual passwords are not shared. When My Concern at the highest level is viewed, all efforts are made to ensure unauthorised individuals are not present and cannot view the contents.	Vicky Dangerfield September 2024 Caroline Powell



Step six - Integrate the DPIA outcomes back into the key documentation

Vicky Dangerfield and Caroline Powell are responsible for integrating the DPIA outcomes back into the key documentation and are responsible for implementing the solutions that have been approved.			
Action to be taken/DPIA outcomes	Key Documentation	Date for completion of actions	Responsibility for actions
My Concern contract and privacy notice checked	Contract Privacy Notice	November 2019	Vicky Dangerfield and Caroline Powell
CP lead to check accuracy by running reports periodically	My Concern guidance documentation	January 2020	Vicky Dangerfield and Caroline Powell
Passwords for individuals with rights based on access, password are not to be shared.	My Concern guidance documentation Data Protection Policy Staff acceptable use policy Staff training	Ongoing	Vicky Dangerfield and Caroline Powell



Annex B Linking the DPIA to the General Data Protection Principles

This annex will help you identify where there is a risk that the initiative will fail to comply with the General Data Protection Regulation or other relevant legislation. The principles listed are those set out in Article 5 of the General Data Protection Regulation with italic notes explaining the information you need to consider.

NB - The wording refers to projects using a broad definition and for the purposes of conducting a DPIA should be applied to any initiative.

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Are your actions a proportionate response to the need?

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');



Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

In addition to the Principles in Article 5, Chapter V covers data being transferred to another country outside the European Economic Area

Will the project require you to transfer data outside of the EEA?