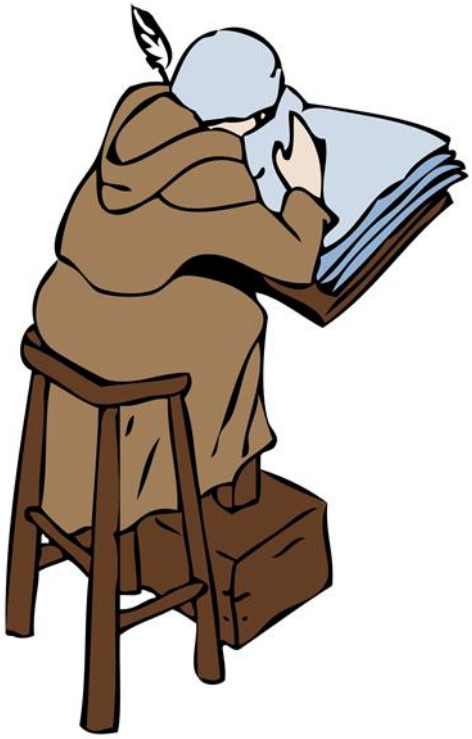

St Bede's RC VA Primary, Jarrow

GDPR/DPA 2018 - Data Protection Policy

Head Teacher – Mrs M Rooney
St Bede's RC VA Primary School
Harold Street
Jarrow
NE32 3AJ
Tel 0191 489 8218

Contents

Introduction

The following documents are used by the school to demonstrate compliance regarding the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018).

The school as part of their GDPR/DPA2018 process also have a personal data ecosystem which includes a data risk register. The personal data ecosystem alongside these documents are working documents and will be reviewed on a regular basis.

The data protection officer for the school is Bryan Chapman of Chapman Data & Information Services LTD.

The school is registered with the ICO. This registration will expire on 16 January 2020

Data Protection training was provided to staff members on 30 April 2018

Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and/or share include:

- Personal information (such as name, unique pupil number and address, adult emergency contact information)
- Characteristics (such as free school meal eligibility, Pupil Premium Information)
- Special Categories (such as Ethnicity, Language, Nationality, Country of birth & Religion)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information (Special Category Data)
- Special Educational Needs information
- Exclusions and Behavioural information.
- Financial Information (such as dinner money transactions, trip transactions)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- Financial audits
- to provide a rewards structure
- to track how well the school is performing as a whole

The lawful basis on which we use this information

We collect and use pupil information under the Education Act 1996/ Data Protection Act 2018 and EU General Data Protection Regulation **(**GDPR**)** Article 6, and Article 9 -from 25 May 2018.

Special category data from article 9 is processed under condition (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purpose, except where Union of Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. This will be via the pupil information sheet that you are requested to complete upon your child's entry to the school.

Storing pupil data

We hold pupil data if it is lawful for us to do. Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's GDPR Data Ecosystem document.

Who we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- Medical information as appropriate/necessary with the NHS
- Third party companies/partners who are assisting the school. All third-party companies/partners who process data on our behalf will have a data processing agreement with the school.

Why we share pupil information

- We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

- We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

- We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

- We share data with schools that your child attends after leaving us to assist with the school transition process.

- We share data with third party companies/partners who may require this information to assist the school.

- We share pupil data with the NHS when appropriate to assist with medical needs of children within the school.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics

- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the school. Please see the schools subject access request policy for further information.

You also have the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress
· prevent processing for the purpose of direct marketing
· object to decisions being taken by automated means
· in certain circumstances, have inaccurate personal data rectified, restrict processing, erased or destroyed
· Data portability
· claim compensation for damages caused by a breach of the Data Protection regulations; and
· Withdraw consent for special categories by requesting a new pupil information sheet

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office: · Report a concern online at https://ico.org.uk/concerns/

· Call 0303 123 1113

· Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact the data protection officer by e-mail (below) or contact the school who will pass your details to the data protection officer.

Bryan Chapman
Chapman Data and Information Services Ltd
dpo@chapmandis.co.uk

Privacy Notice (How we use School Workforce Information)

The categories of workforce information that we collect, hold and/or share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information (such as gender, age, ethnic group)
- contract information (such as start dates, hours worked, post, roles, payroll and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- Performance management data (such as appraisal/observation records)
- Medical information
- Addresses

Why we collect and use this information

We use the school workforce information to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Provide access to third party solutions to dispense your professional duties
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

The lawful basis on which we use this information

We process this information under the Education Act 1996 (departmental censuses), Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) Article 6, and Article 9 - from 25 May 2018

Special category data from article 9 is processed under condition (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purpose, except where Union of Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

Collecting your information

Whilst the majority of the information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this. This will be via an employee information sheet.

Storing this information

We hold school workforce data if it is lawful for us to do. Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's GDPR Data Ecosystem document.

We routinely share workforce information with:

- our local authority
- the Department for Education (DfE)
- Third party companies/partners who are assisting the school. All third-party companies/partners who process data on our behalf will have a data processing agreement with the school.

Why we share workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, staff have the right to request access to information about them that we hold. To make a request for your personal information, contact the school. Please see the schools subject access request policy for further information.

You also have the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress
· prevent processing for the purpose of direct marketing
· object to decisions being taken by automated means
· in certain circumstances, have inaccurate personal data rectified, restrict processing, erased or destroyed
· Data portability
· claim compensation for damages caused by a breach of the Data Protection regulations; and
· Withdraw consent for special categories by requesting a new pupil information sheet

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office: · Report a concern online at https://ico.org.uk/concerns/

· Call 0303 123 1113

· Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact the data protection officer by e-mail (below) or contact the school who will pass your details to the data protection officer.

Bryan Chapman
Chapman Data and Information Services Ltd
dpo@chapmandis.co.uk

Data Breach Policy

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

It is a security incident that has affected the confidentiality, integrity or availability of personal data. Whenever a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

The ICO must be informed if the breach has resulted in a risk to people's rights and freedoms; if this is unlikely then it does not have to be reported. However, if the breach has not been reported then the school should be able to justify this decision.

In assessing if a data breach has created a risk to people's rights and freedoms then Recital 85 of the GDPR should be consulted.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

If a data breach has occurred and this has been caused by a member of staff, the member of staff could be required to undertake additional training or this could lead to disciplinary action, including dismissal, depending on the nature of the breach.

Data Breach Process

1. Data Breach reported to either head teacher or school data protection officer. Whichever is informed, they will inform the other with immediate effect.

2. Immediate action taken to contain the breach.

3. Begin completion of the data breach document log by Data Protection Officer.

4. Any actions from data breach document log carried out.

5. Chair of Governors to be informed in a timely manner.

6. Completed data breach document log agreed by both Head Teacher and Data Protection Officer and copies kept by both.

Staff Data Processing Agreement

For the use of this document data is defined as Personal Identifiable Information (PII) or confidential information.

I agree to;

1. Never disclose or share any data to anyone who should not have access.
2. Never openly discuss data in an environment where it may be possible that a third party could overhear.
3. Destroy/delete any data that I have no lawful reason for holding.
4. Shred any paper documents that I no longer require that contains data.
5. Never willingly access data that I have no right to access.
6. Never willingly alter data without permission.
7. Never save data on a laptop/desktop and will always save data in the agreed locations on the network within the school.
8. Use memory sticks in accordance with the school policy.
9. Lock my computer when I leave my workstation.
10. Log out of all systems when not in use.
11. Never send data in an e-mail unless it is secure.
12. Report any concerns around data to either the school leadership or the data protection officer for the school.
13. Report any personal data breaches in accordance with the school's data breach policy.
14. Never leave data on my desk while not in attendance (clear desk policy)
15. Never share passwords.
16. Never log into a system using another person's log in.
17. Never print data unless necessary.
18. Adhere to the laws governing The General Data Protection Regulation (GDPR).

Failure to comply with the above, could lead to a data breach investigation in accordance with the school's data breach policy, which has been given to you with this document.

Signature_____

Print Name_____

Date_____

Email Policy

Retention of Emails

All Emails will be kept by the school no longer than is necessary for the purpose of which the personal data are processed.

Emails will be deleted by the school **1 Year** after they have been received or sent. However, certain Emails may be kept for longer periods (including indefinitely, if this is in the best interest of the school). Each deletion period will occur at the beginning of each month.

If requested the school will be able to provide justification for any Emails stored after the above time period.

BCC (blind carbon copy)

If any Emails are sent by the school to more than one individual, then the school will use BCC. This ensures that the names of the recipients are kept private and no one within that Email will receive the email addresses of anyone else.

Confidential and sensitive information

No Emails containing confidential or sensitive information will be sent by the school unless this is by a secure manner. This will include items such as children's names and any data that is subject to Special Category protection under GDPR.

Confidential and sensitive information excluding the above list would be determined by the school.

Marketing

Marketing emails will not be sent by the school to any party who has not opted-in to receive such Emails.

The School email services are provided by **Realsmart**

Data Protection by design and default policy

Under the General Data Protection Regulation (GDPR), the school has a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Privacy by design should be a key consideration in the early stages of any project and should continue throughout its lifecycle. This allows schools to minimise privacy risks and builds trust. By designing projects, processes, products and systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage.
- Increased awareness of privacy and data protection across the school.
- The school are more likely to meet their legal obligations and less likely to breach GDPR.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

There are 7 foundational principles of privacy by design

- Proactive not reactive
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – Positive-sum, no zero-sum
- End-to-End security – Full lifecycle protection
- Visibility and transparency
- Respect for user privacy

1. **Proactive not reactive**

   The Privacy by design approach is characterised by being proactive rather than reactive. By using this approach, the school will anticipate and prevent privacy invasive events before they happen. This approach means that the school are not waiting for a privacy risk to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short privacy by design comes before the fact, not after.

2. **Privacy as the default setting**

   Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy.

3. **Privacy embedded into design.**

   Privacy by design is embedded into the design of school practices. It should not be a bolted add on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy becomes integral to school practices.

4. **Full Functionality – Positive-Sum, not Zero-Sum**

   Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

5. **End-to-End security – Full lifecycle protection**

Privacy by design, having been embedded into the project prior to anything else extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, privacy by design ensures cradle to grave, secure lifecycle management of information, end-to end

6. **Visibility and transparency**

Privacy by design seeks to assure everyone that whatever the practice of the school regarding personal data that it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. **Respect for user privacy**

Above all, privacy by design requires the school the protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy Impact Assessment (PIAs) Policy

Privacy Impact Assessments (PIA's) are an integral part of taking a privacy by design approach. PIA's are a tool that the school can use to identify and reduce the privacy risks of a project. A PIA can reduce the risk of harm to individuals through misuse of their personal information. It can also help the school design a more efficient and effective process for handling personal data.

You can integrate the core principals of the PIA process with your existing project and risk management policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout the school.

An effective PIA will allow the school to identify and fix problems at an early stage and PIA's are an integral part of privacy by design. PIAs are often applied to new projects. However, a PIA can also be used if the school are planning changes to an existing process.

The school have a process and guidance on how they will approach PIAs.

Privacy Risk

PIA's should assist the school in identifying privacy risk, which is the risk of harm through an intrusion into privacy. This is the risk of harm through use or misuse of personal information. Some ways that this risk can arise are through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

The outcome of a PIA should be to minimise privacy risk. The school should develop an understanding of how it will approach the broad topics of privacy and privacy risk.

Benefits

The benefits of a PIA are that allows individuals to be reassured that the school which uses their information have followed best practice. A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way. A PIA should also improve transparency and make it easier for an individual to understand why their information is being used.
The school should also benefit from using PIA's. The process of conducting the assessment will improve how the school use information which impacts on individual privacy. This should in turn reduce the likelihood that the school will fail to meet its legal obligations.
Conducting and publishing a PIA will help the school build trust with the people using their services. The actions taken during and after the PIA process can improve the schools understanding of its stakeholders.
Consistent use of PIA's will increase the awareness of privacy and data protection within the school and ensure that all staff involved in designing projects think about privacy at the early stages.

When should we use PIAs?

The core principals of PIA can be applied to any project that involves the use of personal data, or any other activity which could have an impact on the privacy of individuals.
A PIA should be used on new projects or when making an amendment to a current project. The PIA should be built into the project management structure.

Who should carry out the PIA?

It is the school decision who is best placed to carry out the PIA. The Data Protection Officer (DPO) is well placed to have a significant role in a PIA. However, the PIA is designed to be used by anyone within the school. For the PIA to be effective it should include some involvement from various people within the school, who will each be able to identify different privacy risks and solutions.

What should the PIA do?

The PIA should be flexible so that it can be integrated with the schools existing approach to managing projects. The PIA should incorporate the following:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process.

PIA Document Log

Screening questions to assess if a PIA is required

If the answer is yes to any of the questions below, then using a PIA may be useful.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to this information?
- Are you using the information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve using new technology which might be perceived as being privacy intrusive?
- Will the project result in the school making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, use of special category data within GDPR.
- Will the project require you to contact individuals in ways which they may find intrusive?

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Data Flow

- How is the information collected?
- How is the information stored?
- How is the information used?
- How is the information deleted?

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here, and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Privacy Risks

- Are there any privacy risks to individuals?
- Are there any compliance risks to the school, such as fines for non-compliance?
- Are there any school level risks?

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.
Consultation can be used at any stage of the PIA process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy Issue	Risk to individuals	Compliance Risk	Associated organisation/corporate risk

Step four: Identify privacy solutions

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

Risk	Solution	Result – Risk has been eliminated/reduced, or accepted	Evaluation – Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Consent Process

Sought

- For new pupils a consent form should be given to parents/carers before the child begins at the school.
- The school adopts a positive opt in approach to its consent. This means that should a parent/carer not return a consent form or leave any aspect of the consent form incomplete then the school will take this as a no.

Recorded

- When a parent/carer returns their consent form. This information should be entered into your School MIS.
- The consent form should then be filed away in a secure location for future reference if required.
- The consent form is being kept owing to it having the parent/carers signature which will allow the school to verify consent should they be challenged.

Managed

- Consent will be reviewed annually. For current pupils an updated consent form should be given once a year. By doing this it gives parents/carers a real choice in controlling their consent.
- If a parent/carer does not return an updated consent form when requested, then point 2 (sought) would apply.
- The school will ask for very clear and specific consent for information not on the school consent form, should they require it, e.g. one-off events. This will be carried out using the same processes within this document.
- Any third-party controller who the school seek consent on behalf of will be named.
- If a parent/carer wishes to withdraw consent, they would contact the school and request a new consent form.
- This form will be sent out in a timely manner, and the School MIS updated accordingly.
- The new consent form will be filed with previous versions.
- Previous versions are being kept owing to them having the parent/carers signature which will allow the school to verify consent should they be challenged.
- Consent forms will be destroyed in accordance with the school personal data ecosystem.
- The school will avoid making consent a precondition of a service unless there is a lawful requirement to do so.

Subject Access

If the school receive a subject access request from an individual, they will follow the procedure listed below.

1. The school will contact the Data Protection Officer in the event of a subject access request and the Data Protection Officer will assist the school throughout the process.
2. The DPO will inform the school of the steps required to be carried out in regard to the Subject Access Request.
3. The school will first establish who the individual is making the request on behalf of. Is it access to their own personal data or is it on behalf of someone else?
4. The school will then establish if the individual has a valid reason for accessing the data. ICO guidelines state that they are not entitled to the information just because they may be interested.
5. If a valid reason is forthcoming, then the individual will be asked to make the request in writing. E-mail, fax and under certain circumstances social media are all acceptable for the subject access request to be a valid one.
6. The school may be allowed to charge a fee for the subject access request, and this will be communicated back to the individual if this is the case. However, this is unlikely, and the school will contact the DPO for further advice.
7. The school are not required to respond to verbal request. However, depending on the circumstances, it could be reasonable to do so, if the school are satisfied about the person's identity.
8. Should the individual requesting the data be disabled and they find it impossible or unreasonably difficult to make the request in writing, then the school will make reasonable adjustments under the equality act of 2010.
9. Even if the subject access request does not mention that it is a subject access the school will treat it as such, if it is clear that the individual is asking for their own personal data (or on behalf of someone else).
10. The subject access request will be treat as valid by the school regardless of who it has been sent to within the school.
11. The school will then establish if the information requested falls within the definition of personal data.
12. Once a valid subject access request has been received. The school will determine the nature of the request, and a decision will be made on what information can be provided if the subject access request relates to a child, and the time scales to adhere too. *GDPR states 1 calendar month for a request. However, ICO guidelines state 15 school days for a child's educational records.*
13. The school will provide the data as it was at the time of the request. Unless the routine use of the data has led to it being amended or even deleted. In this case the school would supply the information that it holds when the response is sent to the individual even if this is different to that held at the time of the request.
14. However, the school will not amend or delete any data during a subject access request that it would not have otherwise done so.
15. The school will provide the information to the individual in an 'intelligible form'. This means that it will be provided in a way that is capable of being understood by the average person.
16. The school may request more information about the subject access request if they are not satisfied that the person making the request is the individual to whom the personal data relates (or on behalf of), or the school may ask for information that the school reasonably needs to find the personal data covered by the request.
17. If the subject access request is made on behalf of a child, then the school will consider whether the child is mature enough to understand their rights and if so, the school will respond to the child not the parent. However, when considering borderline cases other factors will be taken into account.
18. The school will not comply with a subject access request if by doing so would mean disclosing information about another individual who could be identified from the

information provided. Unless, the other individual has given consent, or it is reasonable in the circumstances to comply with the request without the individuals consent.

GDPR Individuals Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right of erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The school will ensure that all parents/carers and school staff are aware of these rights via the school privacy notices. Also, the school will ensure that should any parent/carer or member of school staff request to invoke any of the rights listed above, that they will treat the request in the correct manner and assist the individual anyway it can.

However, some of the rights listed will not apply due to other conditions set. An example would be the right to erasure, as if the individual requested this to happen to a record, then this could hamper the school's ability to perform its public task. As such, any requests that are made will be treat on a case by case basis, and the requester will be kept informed at all times around the decisions that the school make regarding their request.

Below is a brief guide to what each of the rights are:

1. **The right to be informed** – The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

2. **The right of access** – Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. **The right to rectification** – The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.

4. **The right to erasure** – The right to erasure is also known as the 'right to be forgotten'. The broad principal underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. **The right to restrict processing** – Individuals have the right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

6. **The right to data portability** – The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. **The right to object** – Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise or official authority (including profiling). Direct Marketing and processing for purposes of scientific/historical research and statistics.

8. **Rights related to automated decision-making including profiling** – This is not applicable to schools. However, should an individual challenge the school in any way regarding automated decision making, then the school will carry out an investigation.

Vital Interests

GDPR has the following lawful bases for processing data:

(d) Vital interests: the processing is necessary to protect someone's life.

This is one of the lawful bases that the school uses for processing data within GDPR. It is required as the school processes the personal data to protect someone's life

This processing is necessary as without it the school would not be able to protect a person's vital interests in any other less intrusive way. The school rely on this basis to store medical and special educational needs data to assist the school in protecting someone's life.

Article 6 (1) (d) provides the lawful basis for processing where:

'Processing is necessary in order to protect the vital interests of the data subject or of another natural person'

Recital 46 provides further guidance:

'The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principal take place only where the processing cannot be manifestly based on another legal basis.'

This lawful basis generally only applies to matters of life and death. This is likely to be relevant for emergency medical care. While the school will use lawful basis **(a) consent: the individual has given clear consent for you to process their personal data for a specific purpose**, for the majority of its medical and special education needs processing. It may be required to use vital interests in the case of a life and death matter.

3rd Party Processing Agreement

STANDARD FORM CONTRACT TO ASSIST COMPLIANCE WITH OBLIGATIONS IMPOSED BY ARTICLE 17 OF THE DATA PROTECTION DIRECTIVE 95/46/EC

(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS LOCATED WITHIN THE EUROPEAN ECONOMIC AREA WHERE THE PARTIES HAVE ENTERED INTO A SEPARATE DATA PROCESSING AGREEMENT)

THIS AGREEMENT is made on [ ] 200[ ] BETWEEN:

(1) [NAME] (incorporated in, or existing and established under the laws of, [COUNTRY WITHIN THE EEA] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Controller"); and

(2) [NAME] (incorporated in, or existing and established under the laws of, [COUNTRY WITHIN THE EEA] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Processor").

BACKGROUND

(A) The Controller processes Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of other businesses and organisations;

(C) The Controller wishes to engage the services of the Processor to process personal data on its behalf;

(D) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

(E) Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;

(F) In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the Controller and Processor wish to enter into this processing security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"Data Protection Directive" shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"national law" shall mean the law of the Member State in which the Processor is established;

"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"sub-contract" and "sub-contracting" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

"Technical and organisational security measures" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

2. CONSIDERATION

2.1 In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2 The Processor shall take such Technical and Organisational Security Measures as are required under its own national law to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Agreement.

4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. SUB-CONTRACTING

5.1 The Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Controller.

5.2 Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

5.3 For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

6. TERM AND TERMINATION

6.1 This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.

6.2 Within [ ] days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

7. GOVERNING LAW

7.1 This Agreement shall be governed by and construed in accordance with the national law of the Member state in which the Controller is established

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

(Authorised signatory)

(Print name and title)

SIGNED on behalf of [PROCESSOR]

(Authorised signatory)

(Print name and title)

Freedom of Information Publication Scheme

Information to be published. This includes datasets where applicable - please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 1- Who we are and what we do *(Organisational information, structures, locations and contacts)* *This will be current information only*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Who's who in the school	School Website Hard copy	Free 10p per sheet
Who's who on the governing body / board of governors and the basis of their appointment	School Website Hard copy	Free 10p per sheet
Instrument of Government / Articles of Association	School Website Hard copy	Free 10p per sheet
Contact details for the Head teacher and for the governing body, via the school (named contacts where possible).	School Website Hard copy	Free 10p per sheet
School prospectus (if any)	School Website Hard copy	Free Free
Annual Report (if any)	School Website Hard copy	Free 10p per sheet
Staffing structure	School Website Hard copy	Free 10p per sheet
School session times and term dates	School Website Hard copy	Free Free
Address of school and contact details, including email address.	School Website Hard copy	Free Free

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 2- What we spend and how we spend it *(Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit)* *Current and previous financial year as a minimum*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Annual budget plan and financial statements	Hard copy	10p per sheet
Capital Funding	Hard copy	10p per sheet
Financial audit reports	Hard copy	10p per sheet
Details of expenditure items over £2000 – published at least annually but at a more frequent quarterly or six-monthly interval where practical.	Hard copy	10p per sheet
Procurement and contracts the school has entered into, or information relating to / a link to information held by an organisation which has done so on its behalf (for example, a local authority or diocese).	Hard copy	10p per sheet
Pay policy	Hard Copy	Free
Staff allowances and expenses that can be incurred or claimed, with totals paid to individual senior staff members (Senior Leadership Team or equivalent, whose basic actual salary is at least £60,000 per annum) by reference to categories	Not Applicable	
Staffing, pay and grading structure. As a minimum the pay information should include salaries for senior staff (Senior Leadership Team or equivalent as above) in bands of £10,000; for more junior posts, by salary range.	Hard copy	Free
Governors' allowances that can be incurred or claimed, and a record of total payments made to individual governors.	Not Applicable	

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 3- What our priorities are and how we are doing *(Strategies and plans, performance indicators, audits inspections and reviews)* *Current information as a minimum*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
School profile (if any) And in all cases: Performance data supplied to the English or Welsh Government or to the Northern Ireland Executive, or a direct link to the data	School Website Hard copy	Free 10p per sheet
The latest Ofsted / Estyn / Education and Training Inspectorate report - Summary - Full report Post-inspection action plan	School Website Hard copy	Free 10p per sheet
Performance management policy and procedures adopted by the governing body.	School Website Hard copy	Free 10p per sheet
Performance data or a direct link to it	School Website Hard copy	Free 10p per sheet
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status	School Website Hard copy	Free 10p per sheet
Safeguarding and child protection	School Website Hard copy	Free 10p per sheet

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 4- How do we make decisions. *(Decisions making processes and records of decisions)* *Current and previous 3 years as a minimum*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Admissions policy/decisions (not individual admission decisions) – where applicable	School Website Hard copy	Free 10p per sheet
Agendas and minutes of meetings of the governing body and its committees. (NB this will exclude information that is properly regarded as private to the meetings).	Hard copy	10p per sheet

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 5- Our policies and procedures *(current written protocols, polices and procedures for delivering our services and responsibilities)* *Current information only. As a minimum these must include policies, procedures and documents that the school is required to have by statute or by its funding agreement or equivalent, or by the Welsh or English government or the Northern Ireland Executive. These will include policies and procedures for handling information requests. In addition, for Wales, this will include a Welsh Language Scheme in accordance with the Welsh Language Act 1993. For Northern Ireland, this will include an equality scheme / statement in accordance with the Northern Ireland Act 1998.*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Records management and personal data policies, including: Information security policies, Records retention, destruction and archive policies, Data protection (including information sharing policies)	Hard copy	10p per sheet
Charging regimes and policies. This should include details of any statutory charging regimes. Charging policies should include charges made for information routinely published. They should clearly state what costs are to be recovered, the basis on which they are made and how they are calculated. If the school charges a fee for re-licensing the use of datasets, it should state in its guide how this is calculated (please see "How to complete the Guide to information").	School Website Hard copy	Free 10p per sheet

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 6- Lists and Registers *Currently maintained lists and registers only (this does not include the attendance register)*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Curriculum circulars and statutory instruments	Hard copy	Free
Disclosure logs	Hard copy	Free
Asset register	Hard copy	Free
Any information the school is currently legally required to hold in publicly available registers	Hard copy	Free

Information to be published. This includes datasets where applicable – please see "how to complete the guide to Information	How the information can be obtained	Cost
Class 7- The Services we offer *(Information about services we offer, including leaflets, guidance and newsletters produced for the public and businesses)* *Current information only*	*Hard Copy* *School Website* *Hard Copy & School Website* *Not Applicable*	
Extra-curricular activities	School Website Hard copy	Free 10p per sheet
Out of school clubs	School Website Hard copy	Free 10p per sheet
Services for which the school is entitled to recover a fee, together with those fees	School Website Hard copy	Free 10p per sheet
School publications, leaflets, books and newsletters	School Website Hard copy	Free 10p per sheet

Additional Information		

Schedule of Charges *This describes how the charges (costs in this document) have been arrived at and should be published as part of this guide.*		
Type of charge – example; costs to school, statutory fee	**Description** – example; postage, photocopying, printing	**Basis of Charge** – example: First class stamp cost, cost of paper and printing *The actual cost incurred by the school
Cost to school	Photocopying/Printing	10p sheet