# Data Protection Policy
# November 2026

To be reviewed: September 2027

## Introduction

The following data protection policy is used by the school to show compliance with the Data Protection Act 2018, sometimes referred to as UKGDPR. **– Updated November 2026**

The school are the data controller and are ultimately responsible for ensuring that they comply with data protection law. The Data Protection Officer role is carried out by Chapman Data & Information Services LTD, whose role is to advise, assist and instruct the school.

Chapman Data & Information Services LTD, cannot be held accountable should the school as data controller fail to follow advice that has been given.

The Data Protection Act 2018 (UKGDPR) puts certain responsibilities upon the data controller such as ensuring they have the correct policies in place, data audits have been carried out, school staff have received basic data protection training, and the school has the correct ICO registration in place.

**It is recommended that this policy is given to every member of staff within the school – This is to ensure that regardless of how a staff member processes data they understand the importance and responsibility they have around protecting personal data.**

**It is also recommended that the school upload this policy to their website.**

The school as data controller will ensure that personal data is kept in accordance with the following key data protection principles:

- Fair, lawful, and transparent processing - Privacy Notice.
- Purpose limitation – Only hold data where required and for its intended purpose.
- Data minimisation – Do not hold data any longer than is necessary.
- Accuracy – Ensure that data is correct.
- Data retention periods – Aware of legal requirements to keep documents. If a document does not come under a legal requirement, then the data minimisation principal should be followed.
- Data security – All reasonable steps will be taken to protect the data the school holds.
- Accountability – To be able to prove that the school adheres to data protection law.

The school's privacy notice has been adapted from the model privacy notice provided by the Department of Education (DFE). This is the minimum requirement expected. However, the school can add to this should they wish.

## Contents Page

Contents

Privacy Notice (How we use your information) ..... 4
Workforce Privacy Notice (How we use your information) ..... 9
Sharing of Data ..... 13
Data Breach ..... 13
Vital Interests ..... 14
UKGDPR Individual Rights ..... 15
3rd Party Processing Agreement (template) ..... 16
Data Protection by design and default ..... 20
Privacy Impact Assessments ..... 22
Consent Process ..... 24
Subject Access Requests ..... 24
Education Records ..... 26
CCTV ..... **Error! Bookmark not defined.**
Photographs and videos ..... 27
Clear Desk & Protecting Data ..... 27
Emails ..... 28
Social Media ..... 29
Biometric Recognition systems ..... 30
Data security and storage ..... 31
Retention ..... 31
School Disposal Guidance ..... 31
Freedom of Information (FOI) ..... 31
Staff Processing Agreement/Acceptable use ..... 31
Bring your own device (BOYD) ..... 31
Cyber Security Responsibilities ..... 32
Artificial Intelligence (AI) ..... 32

# Privacy Notice (How we use your information)

*This notice is aimed at pupils, parents/carers – the school should decide if they pass this notice to the children themselves as well as parents/carers. This would depend on if the child is old enough and mature enough to understand the notice. If you decide to provide this notice to a child, then you should ensure that it is age appropriate.*

**The categories of information that we collect, hold and/or share include but are not limited to:**

- Personal information (such as names, unique pupil number and address, adult emergency contact information)
- Special Categories (such as Ethnicity, Language, Nationality, Country of birth & Religion)
- Characteristics (such as free school meal eligibility, Pupil Premium Information)
- Safeguarding information (such as court orders and professional involvement)
- Medical and administration (such as doctor information, child health, dental health, allergies, medication, and dietary requirements)
- Attendance information (such as sessions attended, number of absences and absence reasons and any previous schools attended)
- Assessment information and attainment (such as key stage 1, key stage 2 and phonics results)
- Relevant medical information (Special Category Data)
- Special Educational Needs information (including needs and ranking)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Financial Information (such as dinner money transactions, trip transactions)
- CCTV – If the school uses CCTV, data will be kept in accordance with the school's CCTV policy
- Biometrics – If the school uses biometrics, this will be processed in accordance with the school's biometric policy

**Why we collect and use this information**

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil attainment progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to keep children safe (food allergies or emergency contact details)
- to meet the statutory duties placed on us by the Department for Education
- 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 your information under the Data Protection Act 2018 (sometimes referred to as UKGDPR), article 6, and article 9.

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.

**Collecting pupil information**

Pupil data is essential for the school's operational use. 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 Data Protection legislation, we will inform you at the point of collection, 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. Also, if applicable data will be taken from your previous school using a common transfer file (CTF).

**Storing your data**

We hold your data if it is lawful for us to do so in accordance with retention guidance taken from the DFE recommended source which is the IRMS toolkit. Should a document not be listed in this toolkit then the school will keep a record of why this data is being retained and will produce upon request. Where the school does not follow the guidance within this toolkit, the school have their own retention document which can be provided upon request.

Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's disposal guidance policy.

**Who we share pupil information with**

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- Our local authority
- the Department for Education (DfE)
- Medical information as appropriate/necessary with the NHS
- If the school is a member of an academy trust, then we may where appropriate share pupil information with the trust.

We also routinely share pupil information with:

Third Party Companies/Partners who are assisting the school or enhancing a child's education. A list of such companies/partners can be provided upon request. These are not added to the privacy notice due to their fluid nature.

- Where required the school will ensure that a data processing agreement is in place.
- We will ensure that a Privacy Impact Assessment (PIA) is carried for any new system that the school acquires.
- We will ensure that if any personal data is transferred to a country that the UK deem to not have adequate data protection laws, that a Standard Contractual Clause (SCC) is in place.
- We will ensure for any system that is online and directed at children will be compliant with the age-appropriate design code (children's code)

**Why we share your information**

- We do not share information about you with anyone without consent unless the law and our policies allow us to do so.
- We share data with schools that your child attends after leaving us to assist with the school transition process.
- We share data with our local authority when it is appropriate to do so to assist in the education of the pupils within our school.

- 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.

**Department for Education**

- 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). Maintained school - under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013. Academies and free schools - under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013. Pupil Referral Units - under regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013
- All data is transferred to the DFE securely and held by the DFE under a combination of software and hardware controls which meet the current government security policy framework. government security policy framework.

**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)**

Much of the data about pupils in England goes on to be held in 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.

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

**Sharing by the Department**

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website:
https://www.gov.uk/government/publications/dfe-external-data-shares

**How to find out what personal information DfE hold about you**

Under the terms of the Data Protection Act 2018, you are entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

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

**How Government uses your data**

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the number of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

**Requesting access to your personal data (Subject Access Request)**

Under data protection legislation, you have the right to request access to information about yourself that we hold. If a parent/carer is requesting data for their child, then this will be provided to the parent/carer unless the school deem the child to be mature enough to understand the data and the subject access process.

The school have 30 calendar days to respond to a subject access request. However, this can be extended by a further two months if required.

To make a request please contact the school.

**Requesting access to your child educational record**

In broad terms an education record would be information that the school holds on a child which is information all about the child and would require no redaction and would follow the child to a new school.

Examples would be attendance, schoolwork, assessment grades, letters to the parents from the school about the child and any other information that the school hold on the child that relates solely to that child.

The school must respond with the information within 15 working school days. To make a request please contact the school.

If the school is an academy, then they are under no obligation to provide this information.

**You also have the right to the following:**

- in certain circumstances to be able 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 (including profiling) and processing for the purposes of scientific/historical research and statistics.
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.
- Have inaccurate/incomplete personal data rectified.
- In certain circumstances restrict processing, request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- a right to seek redress, either through the ICO or through the courts.

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

**Withdrawal of consent and the right to lodge a complaint**

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind or are unhappy with the way we use your personal data then please contact the school.

**Contact**

If you would like to discuss anything in this privacy notice, please contact the school who will in turn contact the school's data protection officer. We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. Version – September 2024

## Workforce Privacy Notice (How we use your information)

*This notice is aimed at staff within the school, school governors and anyone who is carrying out work on behalf of the school where we are required to hold their personal information.*

**The categories of information that we collect, hold and/or share include but are not limited to (where applicable)**

- personal information (such as name, employee or teacher number, national insurance number, address)
- 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

**We use the 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 collect and use your information under the Data Protection Act 2018 (sometimes referred to as UKGDPR article 6, and article 9.

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.

**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 data will be collected upon commencement of your involvement with the school.

**Storing your data**

We hold your data if it is lawful for us to do so in accordance with retention guidance taken from the DFE recommended source which is the IRMS toolkit. Should a document not be listed in this toolkit then the school will keep a record of why this data is being retained and will produce upon request. Where the school does not follow the guidance within this toolkit, the school have their own retention document which can be provided upon request.

Any data that we are no longer required to hold lawfully is deleted/destroyed in accordance with the school's disposal guidance policy.

**Who we share your information with**

We routinely share information with:

- Our local authority.
- The Department for Education (DfE)
- If the school is a member of an academy trust, then we may where appropriate share pupil information with the trust.

Third Party Companies/Partners who are assisting the school or enhancing a child's education. A list of such companies/partners can be provided upon request. These are not added to the privacy notice due to their fluid nature.

- Where required the school will ensure that a data processing agreement is in place.
- We will ensure that a Privacy Impact Assessment (PIA) is carried for any new system that the school acquires.
- We will ensure that if any personal data is transferred to a country that the UK deem to not have adequate data protection laws that a Standard Contractual Clause (SCC) is in place.

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)**

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred to the DFE securely and held by the DFE under a combination of software and hardware controls which meet the current government security policy framework. government security policy framework.

**How government uses your data**

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

**Data collection requirements**

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.

**Sharing by the department**

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.

**How to find out what personal information the DFE hold about you**

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

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

**Requesting access to your personal data (Subject Access Request)**

Under data protection legislation, you have the right to request access to information about yourself that we hold.

The school have 30 calendar days to respond to a subject access request. However, this can be extended by a further two months if required.

To make a request for a subject access request please contact the school.

**You also have the right to the following:**

- in certain circumstances to be able 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 (including profiling) and processing for the purposes of scientific/historical research and statistics.
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.
- Have inaccurate/incomplete personal data rectified.
- In certain circumstances restrict processing (i.e. permitting its storage but no further processing), request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- a right to seek redress, either through the ICO or through the courts.

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

**Withdrawal of consent and the right to lodge a complaint**

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind or are unhappy with the way we use your personal data then please contact the school.

**Contact**

If you would like to discuss anything in this privacy notice, please contact the school who will in turn contact the school's data protection officer. We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. Version – September 2024

## Sharing of Data

The school as data controller can share data when requested, but we must have a UKGDPR lawful reason. We will always log our reason. Unless we have a legal obligation to share then we decide which data is sent. Any data we send with be proportionate, and we will challenge why the data is requested if necessary. Data will be sent in a secure manner, and we will only send data regarding the people who the data sharing request is for.

We will request that a PIA is completed by the company/public body you are sharing data with which will assist the school in our decision making. We can also complete a data sharing agreement if we want to put more safeguards in place.

UK GDPR lawful reasons – **We will ensure that the United Nations Convention on the rights of the child that in all actions concerning children, the best interests of the child should be the primary consideration.**

Vital Interest – Sharing data to protect someone's life (life or death situation)

Public Task – In order run the school safely and effectively

Legitimate Interest – (at least one of these four options should be relevant before using this)

1. Is it the best interest of the child such as safeguarding
2. To further the child's education
3. Is in the best interests of the individual
4. To assist in a criminal investigation (non-police)

Legal Obligation – You have a legal obligation to share the data

Contract – You have a contract with the company to share the data. This should never be the sole lawful reason used but is acceptable.

**If the school CANNOT use one of the lawful reasons above, then we understand we MUST get consent or not share the data.**

## Data Breach

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. If reporting is required, then this must happen within 72 hours of the personal data breach being identified (this includes weekends and holidays).

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.

There are several courses of action that can be followed following a data breach. Advice may be given to the individual staff member specifically and/or to school staff in general. This may also result in additional training for an individual, team or whole staff. In the most serious cases and/or when there is evidence to suggest disregard for procedures then this could result in staff receiving a verbal warning, a written warning or potentially dismissal.

The priority for the school is to ensure that the breach is contained.

If the school believe that a data breach has occurred, then they must report this to the Data Protection Officer with immediate effect. The school will then be sent a Data Breach form to complete and return to the DPO which will allow the decision-making process to begin, this in turn will decide if the breach should be reported to the ICO. Upon completion of the data breach form the DPO may advise the school as data controller to either seek further advice from the ICO, or to report the breach to the ICO.

The DPO will recommend that the people whose data has been breached are informed but this decision is ultimately the schools.

Where an individual is informed the school will apologise for the breach and explain the data breach process is being carried out. This will include asking the individual if they wish to complain to the governing body of the school. If the individual is still not satisfied, then the school should contact the DPO to discuss.

The school will adopt a Listen, Log and Learn approach. Listen to the person who has had the breach, Log all the details about the breach, and Learn from the breach to ensure that it does not happen again**.**

## Vital Interests

UKGDPR 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 UKGDPR. 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 principle 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.

## UKGDPR Individual Rights

The UKGDPR 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 any way it can.

However, some of the rights listed will not apply due to other conditions set, as these are not absolute rights. 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 considered 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 (subject Access Requests)** – 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. For further information see Subject Access Requests within this document.

3. **The right to rectification** – The UKGDPR 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 principle 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. However, this is not an absolute right and only applies in certain circumstances. The school has one month to respond to any requests.

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. The school has one month to respond to any requests.

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.

## 3rd Party Processing Agreement (template)

(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS IN ACCORDANCE WITH ARTICLE 28(3) UK GDPR

THIS AGREEMENT is made on (enter month and year) BETWEEN:

(1) (School Name) (incorporated in, or existing and established under the laws of, (enter country) whose registered office is at (School address) (the "Controller"); and

(2) (Enter company name) (incorporated in, or existing and established under the laws of, (Enter country) whose registered office is at (Enter company 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 28(3) of the UK GDPR states that, where processing of personal data is carried out by a processor on behalf of a data controller the controller has an obligation to choose a processor who can provide appropriate security measures, and must ensure compliance with those measures;

Both controllers and processors are obliged to put in place appropriate technical and organisational measures to ensure the security of any personal data they process which may include, as appropriate:

- encryption and pseudonymisation;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore access to personal data in the event of an incident; and
- processes for regularly testing and assessing the effectiveness of the measures.

Adherence to an approved code of conduct or certification scheme may be used as a way of demonstrating compliance with security obligations. Codes of conduct and certification may also help processors to demonstrate sufficient guarantees that their processing will comply with the UK GDPR.

(E) Article 28(3) states 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, the Controller and Processor wish to enter into this processing Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

3. Subject Matter – Enter a brief description of role of the processor.

3.1 Nature and purpose of the processing – Enter a brief description of duties to be carried out by the processor.

3.2 Duration of processing – The processing will continue for the duration of the contract, unless otherwise agreed in writing or required by law.

3.3 Controller's obligations and rights – The Controller is responsible for determining the purposes and means of the processing of Personal Data and for providing documented instructions to the Processor. The Controller has the right to require the Processor to comply with the terms of this agreement and applicable data protection legislation.

3.4 Type of personal data – Enter X where required:

| Children | Children – Special Category | School Staff | School Staff – Special Category | Other | Other – Special Category |
|---|---|---|---|---|---|
| | | | | | |

4. DEFINITIONS AND INTERPRETATION

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

“national law” shall mean the law of the country in which the Processor is established;

“Processor” shall mean all staff in the employment of the company named in section 2.

“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.

5. CONSIDERATION

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.

6. SECURITY OBLIGATIONS OF THE PROCESSOR

6.1 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. As per part 3 of this document.

7. CONFIDENTIALITY

7.1 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.

7.2 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.

7.3 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.

8. SUB-CONTRACTING

The processor shall not engage another processor (a sub-processor) without the controller’s prior specific or general written authorisation;

- if a sub-processor is employed under the controller’s general written authorisation, the processor should let the controller know of any intended changes and give the controller a chance to object to them;

- if the processor employs a sub-processor, it must put a contract in place imposing the same Article 28(3) data protection obligations on that sub-processor. This should include that the sub-processor will provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the UK GDPR's requirements. The wording of these obligations does not need to exactly mirror those set out in the contract between the controller and the processor, but should offer an equivalent level of protection for the personal data; and
- the processor is liable to the controller for a sub-processor's compliance with its data protection obligations.

9. Data Subject Rights

The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, to enable the Controller to respond to requests from data subjects exercising their rights under applicable data protection legislation.

10. Assisting the controller

Under Article 28(3)(f) the contract must say that, taking into account the nature of the processing and the information available, the processor must assist the controller in meeting its obligations to:

- keep personal data secure; notify personal data breaches to the ICO;
- notify personal data breaches to data subjects;
- carry out data protection impact assessments (DPIAs) when required; and
- consult ICO where a DPIA indicates there is a high risk that cannot be mitigated.

11. End of contract provisions

- at the controller's choice, delete or return to the controller all the personal data it has been processing for it; and
- delete existing copies of the personal data unless UK law requires it to be stored.

It should be noted that deletion of personal data should be done in a secure manner, in accordance with the security requirements of Article 32. it is ultimately for the controller to decide what should happen to the personal data being processed, once processing is complete.

12. Audit and inspections

The Processor shall make available to the Controller all information necessary to demonstrate compliance with its obligations under applicable data protection legislation and shall allow for and contribute to audits and inspections conducted by the Controller or another auditor mandated by the Controller.

13. TERM AND TERMINATION

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

13.2 Within (enter number) 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.

14. Additional

This is optional.

School can request further information from the processor – This could be around storage/security, retention, etc, and any other details that the school as the controller would like to ensure are in place. This is to satisfy the controller that the processor is taking care of their data.

While this may encompass some of the points in this document, this section would go into more detail, and can list ALL the different types of data that is being sent.

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)

## Data Protection by design and default

Under the Data Protection Act 2018 (UKGDPR), 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.

Where the school provides an online service likely to be accessed by children, the school will take into account the needs of children when deciding what technical and organisational measures are appropriate to implement data protection by design and by default.

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 it 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 UKGDPR.

- 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 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 Assessments

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.

### 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 it 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?**

The school are responsible for the completion of a PIA. A PIA should be jointly completed by the school and the company if the company will be taking any personal data. This will allow both the school and the DPO to evaluate and make the correct decisions.

If a company do not complete the PIA as requested, by either refusing or directing the school to other documents, then the DPO will not review these documents and the school will have to decide to either accept this or insist as Data Controller that the company complete the PIA. The DPO will only comment on information provided on the PIA and will not review or comment on any other documents. This is following advice given by the Information Commissioner Office (ICO).

Once a PIA has been completed then the DPO will review the PIA and inform the school of any issues or further action to be taken. This will be advice only and it is the school's responsibility as Data Controller to decide to act upon this advice. The school understand they can also complete a data sharing agreement to put more safeguards in place. As Data Controller the school would have to agree this with the company and the DPO would only be able to offer limited advice as this would be unique to the school and the company.

Upon assessment of a PIA the DPO will inform the school of any further requirements and it is the school's responsibility to ensure that this is carried out.

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.

## 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 when the school believe this is appropriate.
- If a parent/carer does not return an updated consent form when requested, then the school will continue to use the previous version.
- 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 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 if required, and the request acted upon accordingly. The school will also accept other forms of written withdrawal and will act upon these requests accordingly.
- The new consent form will be filed with previous versions, should the school feel this is necessary. 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 disposal guidance issued within this document.
- The school will avoid making consent a precondition of a service unless there is a lawful requirement to do so.

## Subject Access Requests

The school, as the data controller, are responsible to ensure that all Subject Access requests are actioned in the correct way and according to UKGDPR. The school, as data controller, are responsible for their completion for all subject access requests and not the DPO.

If the school receive a Subject Access Request (SAR) from an individual, they will action this with immediate effect and without undue delay. This may include the school being satisfied that the individual who is requesting the data is who they say they are. If the school are not satisfied, then they will request identification which will be proportionate.

The school are under no obligation to contact the DPO and can fulfil a request themselves. If this is case, then the DPO will have no input in the SAR process. If the school choose to carry out a request independently of the DPO, they are still able to contact the DPO for advice should this be required. Any advice given should be logged for future reference.

Under the SLA the school have with the DPO there is no requirement for the DPO to carry out anything other than advice regarding a SAR. However, if the school as the data controller inform the DPO and do request full assistance then they will be expected to follow the process and timescales set by the DPO, which means they should inform the DPO immediately when they receive a request. Failure to do so could mean that timescales are missed, and the school could become subject of an investigation by the ICO. This process will inform the school of what is required, in what format and by when. Once the DPO receives the data from the school, then an assessment will be carried out and the school will be informed of any issues.

The DPO will endeavour to complete the SAR on behalf of the school. This may require assistance from the school when necessary. This may include answering questions or assisting in the completion of the request if there are large quantities of data involved. The school should always check the data they receive back from the DPO and should be satisfied.

The school are aware that the SAR must be completed within one calendar month from the date of the request. The timescales are created by using the same date in the following month. Where this is not possible e.g., 31st August, this be complete by the 30th of September. The school understand that this time scale can be extended by a further two months should the request be of a complex nature. If this is the case this will be justifiable, and the requestor will be informed without undue delay and no later than the initial end date given. The end date for a request can be moved if the final day falls on a weekend or bank holiday to the next working day.

The school can clarify a request, as we process a large amount of data. We may ask a requestor to specify the information they require before we respond to a request. This means that we do not have to provide any data until we have obtained clarification. However, we are aware that we cannot force an individual to narrow the scope of their request. If a response is received, then we will action. If a response is not received, we will wait a reasonable period before considering the request closed.

If the DPO carries out completion of the SAR it will be returned to the school with a covering letter for the requestor, and a letter for school use.

The school as data controller: -

- have the right to refuse a SAR should they deem the request to be manifestly unfounded or excessive.
- have the right to charge a reasonable fee in certain circumstances. However, the school understand that in most cases no fee would apply.
- Will not amend or delete any data during a subject access request period, that it wouldn't otherwise have done so in its day-to-day operations.
- Will respond to the SAR in an intelligible form. This means that it will be provided in a way that is capable of bring understood by the average person.
- Consider the rights of a child when a request is made for their data. If the school believe that the child is old enough and mature enough to understand the process and data, then they will refuse the request and explain to the requestor that permission must be sought from the child.
- Will not comply with a SAR if by doing so would mean disclosing information about another individual who could be identified from the information provided, even if the

data is mainly about the person making the request. Unless consent has been given or it is reasonable in the circumstances to comply with the request without the individual's consent. When deciding to not seek consent we will balance the data subjects right of access against the other individual's rights relating to their own personal data. Where a decision is made that consent is not required then justification will be recorded. However, where possible data will be edited to protect the identity of a third party.

- Where we receive a request for CCTV footage then we will carry out a CCTV request assessment in conjunction with the DPO. However, we as data controller reserve the right not to contact the DPO and handle CCTV requests ourselves.
- The school understand that rights of all individuals are to be considered when responding to a subject access request.

## Education Records

An education/School record request is different to a subject access request. However, some information held as part of an education record would cross over into a SAR.

Those with parental authority only can request access to a child's education record under education regulations listed below: -

***In England, schools are regulated by The Education (Pupil Information) (England) Regulations 2005. Those with parental authority can apply to the school to view an education record or receive a copy.***

***In England, this right only applies to all local authority schools and all special schools, including those which are not maintained by a local authority.***

***Independent schools, academies and free schools are NOT OBLIGED to respond to a request for access to a pupil's education record under this legislation.***

***Access to education records is a separate right and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to pupils.***

In broad terms an education record would be information that the school holds on a child, which is information all about the child and would require no redaction. An education record covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher. This is likely to cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body. It may also include information from the child and from you, as a parent, carer, or guardian. The school would decide which information falls within an education/school's records request.

Information provided by the parent of another child or information created by a teacher solely for their own use would not form part of a child's education record.

The school must respond with the information within 15 working school days.

## Photographs and videos

The school will ensure that any photographs/videos used by the school will only be done so with explicit consent from the parent/carer of the child, or any adult included in the photograph/video. It is assumed by the school that this consent will only cover the image of the individual and does not include the publication of names, and any special category data such as gender and date of birth. The school will obtain further consent to use names, and special category data.

This will include photographs/videos;

used in school publications such as newsletters, prospectus;
used on the school website;
used on social media such as Facebook, twitter;
on school premises;
external venues.

The school will make parents/carers aware that while they are permitted to take photographs/videos during school performances/events, that these are for **private use** only, as long as they are not of an indecent nature, and while these can be shared and viewed by friends and family, if they are made available to be viewed by an indefinite number of people then this is likely to no longer be considered a private use and date protection law may apply. Should this be the case the school reserve the right to report the breach of data protection to the Information Commissioners Office (ICO).

Parents/carers will be informed of this policy at every performance/event where the school believe that there is a possibility that photographs/videos could be taken. The school reserve the right to request that no photographs/videos are taken due to safeguarding concerns, which surpasses the parents/carer right to take photographs/videos for their own personal use.

Live streaming of school performances is strictly prohibited.

The above also includes performances/events that are not on the school site but include children and adults who attend the school.

## Clear Desk & Protecting Data

The school will protect personal data and keep it safe from unauthorised access. The school will use a combination of software and hardware controls which may include passwords and encryption.

Also, to improve the security and confidentiality of information, we encourage staff to adopt a Clear Desk Policy approach throughout the school.

This will ensure that all Personal data, is secured when not in use. This will reduce the risk of unauthorised access, loss of and damage to information during and outside of school hours.

This applies to anyone working within the school.

1. Paper documents should be removed from the area, and not left lying around.
2. Items on walls and desks should be justifiable and only done as a last resort. Always, remember that if a document is on a wall or a desk then other people can see it, and this could lead to a data breach.

3. Paper documents must be disposed of in accordance with the school's disposal and retention guidance within this document.
4. Keys for accessing drawers should not be left unattended.
5. Computers should always be locked when unoccupied.
6. Computer equipment which holds personal data will be held securely when not in use.
7. Care should be taken when printing to ensure that documents are not left on the printer unnecessarily. Choose times to do this when the printer may be less busy so the documents can be collected immediately. Under no circumstances should documents not be collected and left on the printer.
8. Use of memory sticks in accordance with the school policy, which is available upon request.

## Emails

### Introduction

Emails and attachments may be confidential and are intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of the school. Communications by e-mail are not guaranteed to be private or secure.

### Usage

All staff have a responsibility to ensure they make appropriate and proper use of emails and to be aware that it is possible that your email may be viewed by individuals other than the intended recipient. Staff should also be aware that not all emails are genuine and that they should not access any emails that appear suspicious. If they are in doubt, they should report to the Head Teacher or their ICT team.

Staff are required to check emails on a regular basis and respond where necessary in a timely manner. When forwarding emails, staff will consider the rights of all individuals included in the email and only forward emails when appropriate.

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. However, the school reserve the right to use CC for multiple email recipients should they believe this is necessary. Where CC is used incorrectly then the staff member will report this as a data breach to the Head Teacher.

Any data that is protected by copyright should not be included in emails.

Staff will always take care to ensure that emails are sent to the correct email address. Should an email be sent incorrectly then the staff member will report this as a data breach to the Head Teacher. Should a staff member receive an email in error then they will report this to the sender immediately and delete from both inbox and deleted folder.

Inappropriate use of email which includes but is not limited to, bringing the school into disrepute, use of offensive, obscene/indecent images or data, hate crimes, defamatory/deceptive comments, harassment, and sending unsolicited emails.

No emails containing confidential or sensitive information will be sent by the staff 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 UKGDPR. Confidential and sensitive information excluding the above list would be determined by the school.

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

Failure to do so could lead to disciplinary action.

**Email Accounts**

If a staff member has unexpected or prolonged absence, then the school is allowed to access their email accounts to ensure that the school is not adversely affected by this absence. The school may also access an email account to fulfill legal requirements under the Data Protection Act 2018 (UKGDPR), and under other circumstances such as but not limited to; prevent and detect crime and protect the school network. Should this occur then approval will be given by the Head Teacher of the school and be justifiable. When appropriate the owner of the email account will be advised of the actions taken by the school.

Where the school allows use of school email for personal use individuals will be informed that they should be aware that the school have the right to access said email should they feel this is necessary and in the best interest of the school. Where this is the case then this will be logged and be justifiable. Personal use of their own email system may take place in an employee's own time provided it does not interfere with the smooth running of the school or deny resources to other users.

**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 month after they have been received or sent. This will be carried out by the staff member or centrally should the school have this facility. However, certain emails may be kept for longer periods (including indefinitely, if this is in the best interest of the school) and will be stored correctly and be justifiable. Each deletion period will occur at the beginning of each month.

The school email service is provided by Microsoft Office 365.

## Social Media

**Definition**

Social Media is defined as websites and applications that enable users to create and share content or to participate in social networking. This includes but not limited to platforms such as Facebook, Twitter, Instagram, Wikipedia.

**Social Media Use**

Staff are expected to keep their personal and professional social media use separate. This is to not only protect them, but the children and parent/carers of the school.

**Basic Principles**

Staff should ensure that data protection principals are always adhered to, and no information relating to personal data should be uploaded to any site unless explicit consent has been given.

Personal data is classified as any information that can identify a living individual or may be possible to identify a living individual. This would include images and videos.

Special category data should never be entered or uploaded to social media. This is data that can be classed as sensitive and could also lead to discrimination against an individual.

No information that the staff member is privy to regarding their role at the school should be entered or uploaded to social media. This would include identifying pupils, parent/carers, or staff at the school.

**Personal social media**

- Staff should not identify themselves as being employees of the school or engage in any activities that bring the school into disrepute, this includes representing your personal views as those of the school.
- Staff should not have social media contact with any pupil unless they are a family member. Unless consent has been given by the school.
- Wherever possible staff should not have contact with a pupil's family member if that contact could constitute a conflict of interest or call into question their objectivity.
- Any personal data as identified in the basic principles section of this document, which in turn identifies the individual as being linked to the school should not be uploaded.
- School email accounts should not be used in creation of social media accounts.
- Social media sites should not be accessed by a staff member during working hours.

**School Social Media**

- Staff should only use social media sites approved by the senior leadership team and used as defined by the senior leadership team.
- Social media sites will be monitored by the senior leadership team.
- When using social media sites on behalf of the school, staff members must always act in the best interests of the children/parent/carers and of the school.

**Misuse**

Any breach of this policy would lead to the school data breach policy being invoked.

**Other**

If the school become aware of comments on social media sites that we believe constitutes a hate crime, then the school reserve the right to report this to the police for action. A hate crime is any crime that is targeted at a person or a group of people because or prejudice or hostility about: -

- Race
- Religion or belief
- Sexual orientation
- Transgender identity – including anyone who is transsexual, transgender, transvestite or who holds a gender recognition certificate.
- Disability – including physical or mental impairment or learning disability.
- Sex

## Biometric Recognition systems

Where the school uses such systems, a full separate policy will be in use and can be obtained upon request.

## Data security and storage

The school will protect personal data and keep it safe from unauthorised access. Computer equipment which holds personal data will be held securely when not in use.

## Retention

The school will only keep documents when we have a lawful reason to do so. The DFE recommend that school use the IRMS toolkit for retention guidance. This or any other retention information can be obtained from the school upon request.

Any documents that are no longer required will be destroyed in accordance with the school's disposal guidance below.

## School Disposal Guidance

All personal data will be destroyed in a robust fashion. This will include shredding paper documents on site by school staff, or where applicable the data being removed by a professional company and destroyed by them either on site or off site. Where a 3rd party company is used then the school will ensure that the correct paperwork is obtained.

Data that is deleted from our computer systems will be destroyed using the technical facilities available to us. Staff members will ensure that data is deleted fully from computer systems.

## Freedom of Information (FOI)

The school is required to have a FOI publication scheme. This lists the documents the school are expected to hold in accordance with ICO model template, and how an individual can obtain these documents. It also lists if the school charge for any of this information, this is accessible on the school website.

The school is under no obligation to have a Freedom of information policy. However, the school will adhere to the legislation regarding FOI as provided by the ICO and respond within 20 school days or 60 working days if this is shorter. Guide to freedom of information | ICO

## Staff Processing Agreement/Acceptable use

All staff members will adhere to the school's staff processing/acceptable use agreement in relation to personal data. This document can be obtained upon request.

## Bring your own device (BOYD)

Where the school allows a staff member to use their own device to process personal data which belongs to the school, then the staff member will adhere to the guidance issued below from the ICO.

https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

## Cyber Security Responsibilities

Schools have a duty to keep personal data safe and protect their digital systems from cyber threats. To do this, they must work closely with their network provider to make sure everything is secure and working as it should. This includes checking that systems like email, internet access, and online learning tools are protected from viruses, hacking, and other risks. Regular reviews and updates are important to fix any issues and keep security strong. Staff and students should also follow safe practices, such as using strong passwords and reporting anything unusual.

The Department for Education has published Cyber Security Standards for Schools and Trusts to help schools understand what good security looks like, and schools are encouraged to follow these as part of their wider data protection efforts.

The DPO's role is to provide advice and guidance on data protection and the security of personal data. The DPO is not responsible for the school's technical cyber-security arrangements, which remain the responsibility of the school and its appointed IT/network provider.

## Artificial Intelligence (AI)

Wherever possible we will seek consent from the data subject before uploading their personal data to an AI system. We will also ensure that we explain clearly what data will be uploaded, and our reasons and justifications for doing so. As per this policy we will follow the guidance regarding seeking consent.

However, we can use other lawful reasons for doing so, and if this is the case, this will be determined before the data is uploaded, and we will log our reasons and justifications for not seeking consent.

Further information regarding the use of AI can be found at the link below and the school will ensure that they always follow this guidance.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/