# Al-Khair Boys' Secondary School

# General Data Protection Policy

| | | | |
|---|---|---|---|
| **Approved by:** | Aisha Chaudhry | **Date:** | April 2019 |
| **Last reviewed on:** | 27.04.2019 | | |
| **Next review due by:** | **April 2020** | | |

## Contents



.....

## 1. Aims

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

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

## 2. Legislation and guidance

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

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

## 3. Definitions

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>● Name (including initials)<br>● Identification number<br>● Location data<br>● Online identifier, such as a username<br>● It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>● Racial or ethnic origin<br>● Political opinions<br>● Religious or philosophical beliefs<br>● Trade union membership<br>● Genetics<br>● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>● Health – physical or mental<br>● Sex life or sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br>Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller |
| Data control breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

# 4. The data controller

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

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

# 5. Roles and responsibilities

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

### 5.1 Senior Leadership Team (SLT)

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

### 5.2 Data protection officer

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

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

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

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

Our DPO is Aisha Chaudhry and is contactable via aisha.chaudhry@alkhairschool.org.uk

### 5.3 Headteacher

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

### 5.4 All staff

Staff are responsible for:

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

# 6. Data protection principles

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

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

# 7. Collecting personal data

## 7.1 Lawfulness, fairness and transparency

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

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

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

## 7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

# 8. Sharing personal data

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

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

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

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

# 9. Subject access requests and other rights of individuals

## 9.1 Subject access requests

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

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

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

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

If staff receive a subject access request they must immediately forward it to the DPO.

## 9.2 Children and subject access requests

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

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

## 9.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

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

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

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

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

### 9.4 Other data protection rights of the individual

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

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

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

## 10. Parental requests to see the educational record

Although this is not statutory for Independent Schools, in the interests of parental collaboration, parents, or those with parental responsibility, can request free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

## 11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to facilities@alkhair.org

## 12. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Uses may include:

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

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

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

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

## 13. Data protection by design and default

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

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

## 14. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or SLT who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## 15. Disposal of records

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

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

## 16. Personal data breaches

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

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

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

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

## 17. Training

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

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

## 18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our

school’s practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full board of trustees.

## 19. Links with other policies

This data protection policy is linked to our Child protection & Safeguarding policy

# Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost ○ Stolen ○ Destroyed ○ Altered ○ Disclosed or made available where it should not have been ○ Made available to unauthorised people
- The DPO will alert the headteacher and the proprietor
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data ○ Discrimination ○ Identify theft or fraud ○Financial loss ○ Unauthorised reversal of pseudonymisation (for example, key-coding) ○ Damage to reputation ○ Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a secure folder in G Drive
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
        - The name and contact details of the DPO
        - A description of the likely consequences of the personal data breach
        - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out: ○ The name and contact details of the DPO ○ A description of the likely consequences of the personal data breach ○ A

description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the: ○ Facts and cause ○ Effects ○ Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals) ● Records of all breaches will be stored in a secure folder in G Drive
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

## Actions to minimise the impact of data breaches

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

***Sensitive information being disclosed via email (including safeguarding records)***

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

We do not share information about you with any third parties that are not listed above without your consent - unless the law requires us to do so.

5 – Where is my data stored?

Some of the data we process is stored on school systems only. Some data may be stored on the systems of organisations that we share data with, which includes cloud-based service providers. Both are managed by Al-Khair Foundation IT Dept. As a school, we enquire from those that we share data with about the processes and policies that providers have in place to ensure that data held on their systems is protected, including where data is transferred outside of the European Economic Area (EEA). There may be international transfer of your data where our suppliers use systems that are hosted in data centres abroad but we always endeavour to ensure that the appropriate privacy protection is in place.

6 – How can I see what data you hold about me?

You have a right to access personal information that we hold about you and can do this by contacting the Data Protection Officer.

MS AISHA
CHAUDHRY
Data Protection
Officer
Al-Khair School
109 Cherry Orchard road
Croydon CR0 6BE aisha.chaudhry@alkhairschool.org.uk 0208 6628664

The data controller responsible for processing your personal data is Folio Education Trust:

7 – For how long do you store data about me?

We follow the guidance of the Information & Records Management Society (IRMS) in determining our data retention policies. Please contact our Data Protection Officer for further information.

8 – What rights do I have regarding my personal data?

- The right to be informed about how your data is used and why. This is the objective of this notice.
- The right of access to see what data is held about you.
- The right to rectification of incorrect or incomplete data held about you.
- The right to erase data if there is no compelling reason for it to be held.
- The right to restrict processing of your data where there is an unresolved dispute about the data.
- The right to object to your data being processed due to your particular situation, if there is no compelling legitimate reason for your data to be processed.
- Rights in relation to automated decision making and profiling.

9 – How do I exercise my rights or make a complaint?

Please contact our Data Protection Officer if you wish to exercise your rights or wish to make a complaint about data-handling. You may also approach the Information Commissioner's Office (ico.org.uk) with your concern.

## Appendix 2: Pupil Privacy Notice

## Privacy notice for pupils at Al-Khair School and their parents and carers

**This document gives you detailed information about how we use your personal data and complies with the Data Protection Act 1998 and the EU General Data Protection Regulations.**

Your privacy is critically important to us. We follow a few fundamental principles as to how we use data:

- We are thoughtful about the personal information that we ask you to provide.
- We carefully consider the ways that we use and store your personal information.
- We share your data only when we need to.
- We take steps to ensure that the organisations with whom we share your information understand that your privacy is critically important.
- We aim to store personal information for as long as we have a reason to keep it and not longer than this.
- We believe in full transparency on how we gather, use, and share your personal information.
- We never sell your personal data to anyone.

1 – Whose data do we process?

We process personal data relating to those who are registered pupils at our school, and their parents and carers. We may also receive data about pupils from a variety of sources including previous schools or colleges, local authority, external agencies such as hospitals, the Department for Education and the Learning Records Service.

2 - Why do we process your data?

As a school, we operate in the public interest to provide all of our pupils with an education, pastoral care and support for their next steps when they leave us. We are also required by law to share some information with the Department for Education (DfE). In order to safely and legally run the school and to meet our legal obligations to the DfE, it is necessary for us to store and process data about both pupils and their parents and carers. If we do not process this data:

- We may be unable to provide pupils with an education or pastoral care.
- We may be unable to keep parents and carers informed about pupil's education and support.
- We may be unable to enter pupils for external examinations or assessments.
- We may be unable to assess the quality of our services.
- We may be unable to meet legal obligations on us as a school or comply with the law regarding data-sharing.

In addition to this, we may contact all parents/carers to make a voluntary contribution towards funding of the school and have a legitimate interest in doing so. All voluntary contributions are used towards the running of the school to the benefit of all pupils. We also retain alumni details and our school buildings may include alumni photographs and displays of past pupils' achievements. We have a legitimate interest in storing this data to help maintain and conserve the past history and culture of the school.

Your data is processed for the following reasons:

- Supporting and managing the learning needs of our pupils
- Providing appropriate pastoral care and meeting pupils' welfare needs

- Complying with requirements set by bodies which manage the awarding of external qualifications to our pupils (such as OFQUAL or individual examination boards)
- Monitoring and reporting on pupil progress
- Offering career guidance and access to training providers
- Enabling parents and carers to be kept informed about their children's education
- Assessing the quality of our services
- Administrating and running educational trips and visits
- Undertaking fundraising for the school through sending out PTFA communications
- Maintaining accounts, running of the school and management of school property
- Complying with laws on data-sharing, safeguarding and children missing from education
- Ensuring security and preventing crime through the use of CCTV

The data that we require about your child includes some sensitive data.

*Sensitive data that we **must** know about*

- You ***must*** tell us about a pupil's health or medical conditions.
- As a school, we operate in the public interest to educate children. We must provide the right level of care and support for all of our pupils. We would be unable to keep children safe without processing some essential health-related information to enable us to do that.
- If we were unable to store or process this information, we would be unable to meet the learning or welfare needs of our pupils.

*Sensitive data that you **do not have to share** with us*

- Some sensitive data is shared with us ***optionally*** e.g. ethnicity**.** This data is held and processed only because both pupil and parent or carer have consented and agreed to share this data with us.
- You do not have to share this with us. You can change your preference at any time by contacting the school. You can also request for this to be deleted and in doing so, this will not affect our ability to provide your child with an education.

3 – What data do we process about pupils and families?

The personal data that we hold and process may include:

- Personal details, including names, child's date of birth, home address, parents and carers contact details, pupil photographs, passport numbers and unique learner numbers
- Personal characteristics (such as ethnic group, religion, disability, medical impairments, country of birth, language, free-school meal eligibility, looked-after status and special needs)
- National curriculum assessment results
- Attendance and absence information
- Pastoral welfare, behaviour commendations, disciplinary incidents and exclusions information within our school (and any similar information received from previous school files)
- Leavers' destinations and alumni contact details
- Photographic, audio or video material of pupils (where required for pupil assessment)

4 – How do we share your data?

Information sharing takes place on a routine basis as part of our usual school processes.

- The first table below summarises how data may be shared with third parties, including which data is shared and why it is shared.
- In exceptional or extraordinary circumstances, there may be cases where additional information is shared about a particular pupil and these are detailed in the second table.

**TABLE 1 - ROUTINE SHARING**

| Who Data is Shared With | What Data is Shared | Reason for Sharing |
|---|---|---|
| Local authority – School admissions | Pupil name, date of birth, home address, parent or carer details, school application reference number and unique pupil number | To administrate school admissions |
| Local authority - Youth support service | Pupil name, address, date of birth, names and addresses of parents and carers | To meet legal requirements. Parents can request sharing is restricted to pupil's name, address and DOB. |
| Local authority – Health & safety Department | Pupil name, date of birth, home address, parent or carer telephone details | To track incidents where an accident form was completed after a health and safety incident involving a pupil or member of staff |
| Local authority – Education department | Pupil name, date of birth, address, date of leaving and destination, attendance marks, exclusion period and reason and parent or carer telephone details | To comply with legal obligation on the school to share information with local authority in respect of safeguarding, promoting welfare and reporting children missing from education |

| | | |
|---|---|---|
| Department for Education (DfE) | All census data fields as listed in Department for Education (DfE) document | We are required to provide information about you to the DfE as part of data collections such as the school census. Under the Education Act 1996, the DfE requires all schools to submit data about all pupils and the school staff as part of a termly census.<br>Some of this information is then stored in the DfE's National Pupil Database, which provides evidence on how schools are performing. This, in turn, supports research. The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.<br>The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data. |
| Careers guidance provider – Independent advisor | Pupil name, email address, action plan | To provide career guidance to pupils |

| Who Data is Shared With | What Data is Shared | Reason for Sharing |
|---|---|---|
| Examination boards (AQA, Edexcel/Pearson, JCQ,) | Pupil name, date of birth, special educational needs and/or personal circumstances which may affect exam performance; audio and/or visual images or recordings where they are required for assessment in a particular subject. | To assess the pupils' exam performance |
| Other schools when a pupil transfers | A standard transfer file sent is securely via the Department for Education (DfE)'s designated web service | To pass on information to a destination school or college when a pupil transfers |
| Travel companies | Pupil name, date of birth, passport details if relevant, medical issues, dietary requirements, next of kin contact details | To administrate school trips and visits |
| Cashless payments provider - ParentPay | Pupil name, parent or carer email address, date of birth, gender, religion, free school meal entitlement, home address, parent or carer DOB | To enable the school to operate payments electronically for services such as lunches or school trips |
| HMRC | Parent or carer's name, house number and postcode | To claim Gift-Aid on donations made to school by parents and carers |
| Photography - Bentley Photography | Pupil name, visual image | To take photographs of pupils in school |
| School Nursing Provider – NHS provider | Pupil name, date of birth | To administer and undertake immunisation programme |

| | | |
|---|---|---|
| Sports events management provider - TeachSPorts | Pupil name and year group | To administrate sporting events for school pupils |
| Parents' evening system provider - School Pod | Pupil name, date of birth, parent or carer name, relationship to pupil, email address and telephone number | To enable parents and carers to book appointments with teachers |
| School management information system provider – Schoolpod | SIMS provides our school system that holds most of our pupil data. This is a cloud-based service which is hosted by SIMS. | To manage and run the school |

| **Who Data is Shared With** | **What Data is Shared** | **Reason for Sharing** |
|---|---|---|
| Homework tracking provider - SMH | Pupil name, unique pupil number, gender, pupil premium, special educational needs, free school meal entitlement, English as an additional language status, first language, year group, pupil email address, parent or carer name, parent or carer email address and parent or carer telephone number | To enable parents and carers, pupils and teachers to track pupils' homework and to provide the school with analysis to assess pupil progress |

**TABLE 2 – INFORMATION SHARING IN EXCEPTIONAL CASES**

| Who Data is Shared With | What Data is Shared | Reason for Sharing |
|---|---|---|
| Local authority – Social services | Pupil name and other information depending on the concern | To follow safeguarding procedures where there is a concern about the safety of a pupil. We have to share information with social services in certain cases to protect children. |
| Police services | Pupil name and other information depending on the concern | To follow safeguarding procedures where there are safeguarding concerns about a pupil;<br>To comply with a request from a law enforcement agency where it may harm their investigation if we do not share information;<br>To seek appropriate pastoral support from the police for students who require it |
| Legal advisors | Pupil name and other information depending on the concern | To gain advice, undertake a legal case or to assist an inquiry or investigation to which the school is a party |
| Local authorities | Pupil name, date of birth | To establish which borough provides funding for a looked-after child, in the exceptional case when the funding borough is not clear |