GDPR Data Protection Policy

1. Introduction

1.1. The 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 UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018.

1.2. This Policy is in place to ensure everyone is aware of their responsibilities and outlines how the School complies with the core principles of GDPR. It applies to anyone who handles or has access to people's personal information, regardless of the way it is used or whether it is in paper or electronic format.

2. Legislative Framework

2.1. This Policy has due regard to legislation including, but not limited to, the following:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000 (FOI)
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998 (SSFA)

2.2. It also has regard to guidance published by the ICO (2018); Guide to the General Data Protection Regulation (GDPR) and to guidance published by the DfE (2018); Data protection: a toolkit for schools.

2.3. The Policy includes the School's Publication Scheme under FOI (attached as Appendix D), the School's policy on CCTV (attached as Appendix E) and the School's policy on Records Management & Information Security (attached as Appendix F).

3. Principles of Processing

3.1. GDPR is based on data protection principles which say that personal data should be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processes in a manner that is incompatible with these purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and 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

3.2. Additionally GDPR requires accountability. The controller needs to be responsible for, and be able to demonstrate, compliance with the principles of processing and the respect for individuals' rights. This Policy sets out how the School aims to do this.

4. Processing of Personal Data

4.1. The School will obtain and process data fairly and lawfully informing individuals of the reason for data collection, the purposes for which data is held, the likely recipients of the data and the individual's right of access. The School will:

- Act in accordance with GDPR by implementing technical and organisational measures which demonstrate how the School has considered and integrated data protection into processing activities and building a data protection approach in all parts of the organisation so that there is a strong culture and everyone routinely asks themselves:
  - Am I required by law to process this data?
  - Do I need to process this data in order to safely and effectively do my job/run this school?
  - Can I share this data?
- Hold the minimum personal data necessary to enable it to carry out its functions and will not hold it for any longer than necessary for the purposes for which it was collected.
- Make every effort to ensure that data held is accurate, up to date and that inaccuracies are corrected as soon as possible.
- Only share personal information with others in ways the individual has been informed about or where it is necessary or where they are required to share and before doing so they will ensure adequate security is in place to protect it and the data recipient has been outlined in a privacy notice or appropriate consent has been obtained.
- Ensure that information disposal is done appropriately and, where necessary, securely.

4.2. Applicable data

Personal Data

Personal data refers to any information that relates to an identified, or identifiable, living individual and includes information such as an online identifier, e.g. an IP address. It applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive Data

Sensitive personal data is personal data, which is more sensitive and includes, but is not limited to, information about an individual such as their race or ethnicity, political opinions, religious beliefs or health.

4.3. Privacy Notices have been drawn up to identify data collected about the School's workforce, volunteers, governors and parents and pupils, how it is used and where it is shared.[1]

- The Privacy Notice for the workforce (including volunteers) is attached at Appendix A
- The Privacy Notice for parents & pupils is attached at Appendix B
- The Privacy Notice for governors is attached at Appendix C

4.4. Data protection and appropriate notices will be integrated into general documentation where appropriate.

4.5. Where data is processed on any other person than those included above the individual will be informed of the lawful reason for collecting the information, how it will be used and their rights in connection with the School holding their data.

4.6. Where data is obtained directly from an individual, information on whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible

[1] Notices may be updated from time to time and any update will not invalidate this Policy

consequences of failing to provide the personal data, will be provided. For data obtained directly from an individual, this information will be supplied at the time the data is obtained.

4.7. Where data is not obtained directly from an individual, information on the categories of personal data that the School holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

4.8. The School does not collect or use biometric data.

5. Data Protection Officer (DPO)

5.1. The School will appoint a DPO who will:

- Inform and advise the School and its workforce about their obligations to comply with data protection law.
- Oversee and monitor the School's compliance with data protection law.

5.2. To do this the DPO will:

- Oversee the development and implementation of this Policy.
- Promote a culture of privacy awareness throughout the school community.
- Ensure that staff, including volunteers and governors, receive appropriate training and advice.
- Undertake periodic audits of the School's data protection processes in action and address any issues arising.
- Ensure individuals are informed of how their data will be used by the School and their rights in respect of the School holding their information.
- Review data impact assessments.
- Ensure that freedom of information requests, subject access requests and other relevant requests are properly dealt with.
- Monitor logs of data breaches and be responsible for reporting as required.

5.3. The DPO will have undertaken appropriate training.

5.4. In this School the DPO is Mr P T Kilbride (Headmaster).

6. Staff Responsibilities

6.1. All staff, including volunteers, are responsible for collecting, storing and processing personal data in accordance with this Policy.

6.2. They are also responsible for informing the School of any change to their own personal data.

6.3. They must contact the DPO for guidance where they:

- Have any questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure.
- Have any concerns that policy is not being followed.
- Are unsure if they have a legal basis for using personal data in a particular way.
- Need to rely on or obtain consent for the use of data.
- Need to transfer data outside of the UK.
- Are sharing personal data with new third parties, or different personal data with existing sharers.

- Are engaging in a new activity, collecting new data types, using data for a different purpose or introducing new processing or software, so that the impact of these can be assessed and, where appropriate, consent obtained or privacy notices adapted to ensure compliance.

6.4. They are responsible for reporting to the DPO any data breaches which have happened through their own actions or where they become aware of one arising from the actions, accidental or otherwise, of others.

6.5. They are responsible for referring all requests for data access, including freedom of information requests, subject access requests and other relevant requests to the Bursar.

6.6. Staff will undertake data handling awareness and data protection training and be made aware of their responsibilities as part of their induction and keep their training up to date in order to comply with GDPR.

6.7. Data protection will also form part of CPD for all staff so that they are fully aware of their responsibilities, of the significance of data protection and how they must comply with its provisions.

7. Lawful Processing

7.1. The legal basis for processing data should be identified and documented prior to data being processed.

7.2. The School will only process personal data where it has one of 6 legal reasons to do so under data protection law and these reasons are where:

- The consent of the individual, or their parent/carer where appropriate, has been freely given; or
- Processing is necessary for:
  - The School to fulfil a contract with the individual, or the individual has asked the School to take specific steps before entering into a contract.
  - The School to compliance with a legal obligation.
  - Protecting the vital interests of the individual or another person e.g. to protect someone's life.
  - The School, as a public authority, to perform a task in the public interest and carry out its official functions.
  - The legitimate interests of the School or a third party provided the individual's rights and freedoms are not overridden.

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

8. Consent

8.1. When the School seek consent the response must be freely given, specific, informed and an unambiguous indication of the individual's wishes. It must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2. Where consent is given, a record will be kept documenting how and when consent was given.

8.3. Consent can be withdrawn by the individual at any time.

8.4. Where a child is under the age of 13, the consent of parents will be sought prior to processing, where appropriate.

8.5. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may

include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted if possible or advised if an immediate on the spot decision was needed.

9. Limitation, Minimisation and Accuracy

9.1. The School will only collect personal data for specified, explicit and legitimate reasons and these reasons will be explained to the individuals when the data is first collected.

9.2. If the School want to use personal data for reasons other than those given when the data was first obtained it will inform the individuals concerned before the data is used and seek consent where necessary.

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

9.4. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised in line with the School's Records Management & Information Security Policy (see Appendix F).

10. Data Security

The School will protect personal data and keep it safe from unauthorised access, alteration or disclosure and against accidental or unlawful destruction or damage. Data is managed in line with the School's Records Management & Information Security Policy (see Appendix F).

11. Publication of Information and Access to Information

11.1. Freedom of information requests (FOI)

The School publishes a 'publication scheme' outlining classes of information that will be made routinely available. A copy of this is attached at Appendix D. The Appendix also explains how an FOI can be made.

11.2. Subject access requests (SAR)

Individuals can request confirmation that their data is being processed and may submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. Information on how to do this is set out in the School's Records Management & Information Security Policy (see Appendix F).

11.3. Other data protection rights of individuals

In addition to the right to make a subject access request as outlined above and to receive information when their data is collected about how it will be used and processed, data protection law gives individuals rights to, for example:

- Ask for the rectification of any inaccurate or incomplete personal data.
- Object and prevent their personal data being used for direct marketing.
- Challenge processing which has been justified on the basis of legitimate interests or the performance of a task in the public interest.
- Object to decisions based solely on automated decision making or profiling.
- Have their data erased where there is no compelling reason for its continued processing.
- Restrict the processing of their data in certain circumstances such as where the data is inaccurate for example.
- Be informed of a data breach in certain circumstances.
- Ask for their personal data to be transferred to a third party so that the individual can obtain and reuse their personal data for their own purposes across different services.

They may also:

- Withdraw their consent to processing at any time.
- Make a complaint to the ICO (see below).

Individuals can submit a request to exercise these rights and information on how to do this is set out in the School's Records Management & Information Security Policy (see Appendix F).

12. CCTV[2] and Photography

12.1. The School understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles. Signs are in place to notify individuals that CCTV is installed.

12.2. The School has a CCTV code of practice and a copy of this is attached as Appendix E.

12.3. As part of our school activities photographs/video footage of individuals or groups of individuals may be taken. It may also do this the purposes of staff training/performance appraisal reviews. These images may be shared internally for the purpose or purposes they were taken however the School will always indicate its intentions to do so and will obtain appropriate consent before publishing them.

12.4. 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. Uses may include:

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

12.5. 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.

12.6. 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.

12.7. 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.

12.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from GDPR.

13. DBS Data

13.1. The School uses the Disclosure and Barring Service (DBS) to help assess the suitability of applications for positions of trust and complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of disclosures and disclosure information. The Code of Practice is intended to ensure and to provide assurance to those applying for disclosures that the information released will be used fairly. The Code also seeks to ensure that sensitive personal information is handled and stored appropriately and is kept for only as long as necessary.

13.2. The School complies fully with its obligations under GDPR pertaining to the safe handling, use, storage, retention and disposal of disclosure information.

[2] Closed circuit television

13.3. In accordance with section 124 of the Police Act 1997, disclosure information is only passes to those who are authorised it receive it in the course of their duties. We maintain a record of all those to whom disclosures or disclosure information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it. Where offences are disclosed, consent is requested from the applicant/employee to retain a copy until it has been assessed by the Headmaster. Throughout this time, usual conditions regarding secure storage and strictly controlled access will apply.

13.4. Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

13.5. Any third parties who access DBS information will be made aware of data protection legislation, as well as their responsibilities as a data handler.

14. Data Sharing

14.1. 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 and where necessary the School will seek consent before doing this
- Suppliers or contractors need data to enable them to provide services to our staff and pupils – for example, catering. When doing this, we will:
    - Only appoint suppliers or contractors who 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

14.2. The School is also legally required to routinely share certain data with relevant authorities including, but not limited to, the DfE, Local Authorities, HMRC and the Border Agency and for purpose which can include:

- The prevention or detection of crime and/or fraud or the apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with the enquiries of investigating and prosecuting authorities for the sole purpose of investigations and/or proceedings
- Where 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

14.3. It may also be shared:

- With pensions providers and insurers where applicable
- With examination boards for entry to external examinations
- Where required in order to enter, or perform under, any contract the School has with the individual
- With the School's professional advisors for the sole purpose of the professional advisors' providing the School with a professional service and on condition that the professional advisors themselves agree not to divulge, publish or use the information
- If required by law or by order of a court of law

- With emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff

14.4. The School use a number of computer applications which are outsourced. Personal data is not publicly shared with these providers but their software uses personal data to enable the School's systems to run (for example email address to facilitate Group Call and pupil data to run the School's information management system) and they have system access in some cases for programme maintenance. The School will carry out assessments to ensure these providers are GDPR compliant.

14.5. Data will otherwise only be shared where the individual has been informed and consent given.

14.6. Data will not be made available to third parties for marketing.

14.7. Data will not be transferred to, or used in, other countries except where it is necessary to do so, for example, because:

- The individual is not resident in the UK
- The individual requests information to be sent to another country
- It is necessary in support of a school activity going to, or in, another country

15. Safeguarding

15.1. The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

15.2. The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

15.3. The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

16. Data Retention

16.1. The School has a responsibility to ensure that records are only kept for as long as is necessary to fulfil the purpose or purposes for which they were intended. Data will not be kept for longer than is necessary and any unrequired data will be deleted/securely disposed of as soon as practicable.

16.2. In determining retention periods the School will have regard to legislation and regulation for each of its records and in certain circumstances there may be reason why even these time scales may need to be exceeded. Retention periods will be informed by the Information and Records Management Society's toolkit for schools.

16.3. Disposal will be managed in accordance with the School's Records Management & Information Security Policy (see Appendix F).

School Policies & Procedures

16.4. If an individual requests erasure of information the School will make every effort to comply however where there is reason not to comply individuals will be advised of this and the reason for this.

17. Data Breaches

17.1. A 'personal data breach' means a breach of security which has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2. The School will make all reasonable endeavours to ensure that there are no personal data breaches however the DPO will ensure that all staff members are made aware of, and understand, what constitutes a data breach and what they must do if this happens.

17.3. All data breaches, whether minor or of greater consequence, must be logged with the DPO who will assess, on a case-by-case basis, the severity of a breach and determine if any personal data is involved and has been compromised. The DPO will implement appropriate containment and recovery measures where necessary. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18. Complaints

18.1. If an employee believes that the School has not complied with this Policy or acted otherwise than in accordance with GDPR, they should utilise the School Grievance Procedure.

18.2. If a parent, pupil or other individuals who are not staff believes that the School has not complied with this Policy or acted otherwise than in accordance with GDPR, they should utilise the School's Complaint Procedure.

18.3. If after going through the relevant grievance/complaint procedure an individual is still not satisfied they may contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

19. How to Contact Us

19.1. Any individual can contact the School in relation to the data the School holds. This includes individuals who wish to exercise any of their rights in relation to personal data processing such erasure or rectification and anyone making a subject access request, a freedom of information request, a grievance claim or a complaint.

19.2. Grievances and complaints should be dealt with in accordance with the relevant policy which sets out who to contact and how to do this. The Grievance Policy is available for staff to access on the School's IT system in the Staff Shared Area as is the Complaints Policy. The Complaints Policy is also published on the Schools website (www.oshsch.com).

19.3. For subject access requests, freedom of information requests and requests in connection with other data protection rights please contact the Bursar using the details below.

Email: lgreen@oshsch.com

Telephone: 01384 817302

Contact address: The Bursar, Old Swinford Hospital, Stourbridge, West Midlands, DY8 1QX.

20. Policy Revision

This Policy is generally reviewed annually but may be reviewed at other times to ensure compliance with current legislation and is therefore subject to change without prior notice.

Privacy Notice

How we use workforce information[3]

Old Swinford Hospital is the Data Controller for the use of personal data in this privacy notice

The categories of school workforce information that we process include

- Personal characteristics and information such as name, address, national insurance number, gender, ethnicity and date of birth
- Contract information such as start date, hours worked, post, roles and salary information
- Bank details
- Identifying documents such as passport numbers, dates of moving home etc., where necessary
- References
- Details of qualifications relevant to your job/role or employment related development and including, where relevant, teacher number and subjects taught
- Contact details such as telephone numbers and email addresses including those delegated to be contacted in case of emergency
- Any relevant medical/disability information and any accident reports
- Records of sickness, appraisal, capability, grievances and disciplinary matters
- Work absence information such as number of absences and reasons
- Data about your use of the school's information and communications systems
- Training records
- Driving information when you either drive a school vehicle or use your personal vehicle for occasional business use
- Vehicle details for those who use the School's car parking facilities
- Enhanced DBS certification and other relevant employment checks
- Photographs & other visual imagery
- CCTV images
- Site/building access information

Why we collect and use this information

We collect and use this data to:

- Establish contractual information
- Establish the right to work in the UK
- Enable individuals to be paid and reporting this to HMRC
- Enable the provision of pensions
- Enable the provision of health insurance where applicable
- Ensure the workforce structure, specialisms and qualifications meets that requirement to provide education to our pupils and caters for their needs and welfare.
- Enable the efficient allocation of resources to meet the needs of the timetable and the provision of boarding and welfare services and support
- Support effective performance management
- Communicate with you

[3] References to the school workforce and staff will include volunteers working in the school

- Inform the development of recruitment and retention policies and of training needs
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Establish identity where a person has to do so relevant to their role e.g. to enable the School's Bank to conform to anti-money laundering regulations
- Inform and help make provision for 'reasonable' adjustment where medical conditions, or disabilities, and other reasons make it necessary for these to be considered
- Comply with security and safeguarding requirements
- Comply with insurance disclosure requirements
- Comply with requirement to share information with a local authority
- Meet the statuary duties placed upon us for DfE data collections including the completion of the school workforce census
- Support site and personal security

The lawful basis on which we collect and process this information under UK GDPR

In order to carry out its duties to staff, to comply with its obligations and duties to meet the purposes of a school and to safeguard its pupils, the School may collect and process a range of personal data about individuals.

Information is required in the first instance for the purposes of recruitment and employment and the School will therefore have a legitimate interest for collecting and processing basic personal data and sensitive personal data.

Thereafter the information it collects and processes will be in order to fulfil its legal rights, duties or obligations including those:

- Under a contract with its staff (lawful basis: contract)
- That ensure and sustain the wellbeing and safety of, and promote the development of, the workforce (lawful basis; legitimate interest)
- That ensure the safeguarding of pupils (lawful basis: vital interest)
- That ensure the statutory needs of the workforce are met and this may include sensitive personal data for health care purposes (lawful basis: legal obligation)
- That meet statutory requirements to provide information to local authorities, the DfE, HMRC and other relevant authorities such as pensions agencies and the School's insurers (lawful basis: legal obligation)

We can also use any information where you have provided your consent (lawful basis: consent)

Collecting information

Most of the information we collect comes from the application and appointment process. Work related information will be added during the time you are working at the School.

Workforce data is essential for a school's operational use and whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with UK GDPR, we will inform you whether you are required to provide certain information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing information

We hold workforce and role related information whilst you are working for the School and then a minimum of seven years from the date of leaving. It may however be necessary to hold this information longer than this where we may be obliged to do so by regulation prevailing at that time.

School Policies & Procedures

Records generated whilst you are working for the School, such as accident records for example, will be kept for the time required under the relevant regulation we have collected it for.

Records generated solely for legitimate reasons whilst you are working for the School will be disposed of when you leave unless we assess, at that time, that they are required for longer by law or regulation or for other reasons. Where this is for other reasons, you will be notified. In respect of any matters of safeguarding information will be kept as long as we require.

Who we share this information with and why

We do not share information about our workforce with anyone without consent unless the law and our policies allow us to do so. We will share information where we are required to do so by law or by order of the court or to prosecuting authorities for the sole purpose of investigations and/or proceedings.

Where we share information, we do so only to the extent that it is required for that purpose.

We are statutorily required to, and routinely share elements of workforce information with:

- The Local Authority
- The Department for Education (DfE)

We are also required to statutorily share elements of workforce information collectively and/or individually with authorities such as HMRC, insurers, pension providers, other regulators such as the Health & Safety inspectorate.

We may be required to share collective information via a Freedom of Information request, but we will do this only as long as individuals cannot be identified.

We will share safeguarding information where necessary and we will do this in an appropriate way.

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

Department for Education
The DfE collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see the 'How Government uses your data' section below. And for privacy information on the data the DfE collects and uses, please see:
https://www.gov.uk/government/publications/privacy-information-education-providers-workforce-including-teachers

Others
We also share some of this information with insurers and other service providers such as banks but only to the extent that it is required to provide cover for the school in respect of its business, activities or its workforce or to the extent that it is required to facilitate the business of the School and for the performance of your duties or to provide an agreed benefit to you.

We will share information where we are required to do so by law or by order of the court or to prosecuting authorities for the sole purpose of investigations and/or proceedings. All staff are reminded that the School is under duties imposed by law and statutory guidance to record and report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, where they meet a certain threshold of seriousness in their nature or regularity. This may

School Policies & Procedures

include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO[4] or police.

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

To find out more about the data collection requirements placed on us by the DfE 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 will only share your personal data where it is lawful, secure and ethical to do so and 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 public benefit, proportionality, legal underpinning and strict information security standards:

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

For information about which organisations the Department for Education (DfE) has provided information, (and for which project) 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 UK GDPR, 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 are 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 or https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

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

Requesting access to your personal data

The UK GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact the Bursar at Old Swinford Hospital.

[4] Local Authority Designated Officer

You also have the right to:

- Be informed about the collection and use of your personal data – this is called the 'right to be informed'
- Ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request, data subject access request or right of access request
- Ask us to change any information you think is not accurate or complete – this is called 'right to rectification'
- Ask us to delete your personal information – this is called 'right to erasure'
- Ask us to stop using your information – this is called 'right to restriction of processing'
- Object to processing' of your information, in certain circumstances
- Withdraw consent at any time (where relevant)

You also have rights in relation to automated decision making and profiling and to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. Examples of some rights not applying include the following:

- Right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- Right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- Right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

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

For further information on how to request access to personal information held centrally by the DfE, please refer back to the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a compliant

Where we are processing your personal data on the basis of consent, you have the right to withdraw that consent. If you change your mind or are unhappy with the use of your personal data, please let us know by contacting the Bursar at the School.

Contact

If you would like to discuss anything in this privacy notice, please contact the Bursar.

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated September 2024.

School Policies & Procedures

Privacy Notice

How we use pupil and parent[5] information

Old Swinford Hospital is the Data Controller for the use of personal data in this privacy notice

The categories of pupil and parent information that we process include

Pupil data

- Personal information such as name, address and date of birth
- Characteristics such as gender, ethnicity, country of birth and language
- Identifiers such as unique pupil number and, where necessary, passport details
- Contact details such as telephone numbers and email addresses
- Eligibility for free school meals, pupil premium, forces premium or other entitlement
- Safeguarding information such as court orders and professional involvement
- Any relevant medical information such as doctors' information, child health, dental health, allergies, medication and dietary requirements
- Welfare information such as referrals to counsellors
- Special educational needs and any relevant education and health care plans
- Personal education plans where relevant
- Previous schools' references, where necessary
- Suitability for boarding assessments
- Attendance information such as sessions attended, number of absences, absence reasons and any previous schools attended
- Curricular and subject choices
- Educational assessment and attainment information such as key stage outcomes, classwork marking, intervention strategies, assessment/examination or test results and destination data
- Behavioural information such as detentions, suspensions, exclusions and any relevant alternative provision put in place
- Attitude to learning assessments
- Extra and co-curricular information including trips, visits and team selections
- Photographic and video images
- Vehicle details for those who use the School's car parking facilities
- CCTV images
- Site/Building access information
- We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education (DfE)

Parent data

- Personal information such as name, address and relationship to pupil
- Proof of address
- Bank details or payment card information where fee payments or school services/clubs are paid for electronically.
- Contact details such as telephone numbers and email addresses including those to be contacted in case of emergency.

[5] Any reference to parent includes carers and guardians

- CCTV images
- Site/Building access information

We may collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Characteristics, such as ethnicity, languages spoken and eligibility for certain benefits
- Family circumstances
- Physical and mental health, including medical conditions
- Support received, including care packages, plans and support providers

We may also hold data about you that we have received from other organisations, including other schools and social services.

Why we collect and use this information

We collect and use this data to:

- Respond to requests for information about joining the School
- Inform the school admissions process
- Support pupil learning
- Monitor and report on pupil progress and attainment
- Enter pupils for examinations
- Provide appropriate pastoral care
- Establish a boarding contract
- Process payments for school services and clubs
- Assess the quality of our services
- Keep children safe
- Support vulnerable children and any other key groups
- Establish funding streams for children with needs
- Comply with requirements to share information with a local authority
- Meet the statutory duties placed upon us for DfE data collections
- Communicate with you
- Keep you informed about the school community and let you know of events
- Support site and personal security

The lawful basis on which we collect and process this information under UK GDPR

In order to meet legal requirements or carry out its duties and its functions the School may process a range of personal data about individuals.

Information is required in the first instance to establish a place in school for each child and the School will therefore have a legitimate interest for collecting and processing basic personal data and sensitive personal data.

Thereafter the information it collects and processes will be in order to:

- Fulfil its duties or obligations to provide education and support and monitor pupils' learning (lawful basis: public task)
- Care and cater for the needs of its pupils, their welfare, wellbeing, pastoral care and their safety and this may include sensitive personal data for health and social care purposes (lawful basis: vital interest)
- Process legal claims or to protect your vital interests and where you are unable to provide

School Policies & Procedures

your consent
- Inform and support the boarding contract (lawful basis: contract)
- Meet statutory requirements to provide information to local authorities and the DfE including pupil data for the school census under the Education Act 1996 (lawful basis: legal obligation)

We can also use any information where you have provided your consent (lawful basis: consent)

Collecting information

We collect information via the registration and admissions process and thereafter by our working with pupils each day in school and in boarding time.

The personal data collected is essential for a school's operational use and whilst the majority of information provided to us is mandatory, some of it requested on a voluntary basis. In order to comply with UK GDPR, 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 and we will tell you what you need to do if you do not want to share this information with us.

Storing information

We hold data securely for the set amount of time required by law or regulation or as otherwise advised in guidance provided by the Information and Records Management Society. For more information on data retention and how we keep your data safe, please read our data protection policy on the School's website.

Records generated solely for legitimate reasons will be disposed of when the pupil leaves school (or after the end of the admissions cycle if the pupil does not attend the school) unless we assess, at that time, that they are required for longer by law or regulation or for other reasons. Where this is for other reasons, you will be notified. In respect of any matters of safeguarding information will be kept as long as we require.

Who we share this information with

We routinely share pupil information with:

- Schools that pupils attend after leaving us
- Local authorities
- Youth support services (pupils aged 13+ and16+)
- The DfE & Ofsted
- The School's doctor (where appropriate)
- Examination boards
- The Combined Cadet Force where applicable
- Duke of Edinburgh and other trip/visit co-ordinators as applicable
- Work experience co-coordinators and assessors
- Suppliers, service providers and professional advisors – to enable them to provide the service we have contracted them for such as, but not limited to, caterers, educational psychologist, SEN assessor etc.
- Services such as the NHS or Police where appropriate
- Colleges and UCAS where references are requested
- The pupil's family and representatives where authorised
- Our School Information Systems providers
- Insurance providers (where necessary)

School Policies & Procedures

We may be required to share collective information via a Freedom of Information request, but we will do this only as long as individuals cannot be identified.

Why we share this information

We do not share information with anyone without consent unless the law and our policies allow us to do so. We will share information where we are required to do so by law or by order of the court or to prosecuting authorities for the sole purpose of investigations and/or proceedings.

We will share safeguarding information where necessary and we will do this in an appropriate way.

Where we share information, we do so only to the extent that it is required for that purpose.

Youth support services – pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to a local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- Youth support services
- Careers advisers

A parent can object to any information additional to their child's name, address and date of birth being passed to a local authority or provider of youth support services by informing us. This right is transferred to the pupil once they reach the age 16.

Youth support services – pupils aged 16+

We will also share certain information about pupils aged 16+ with a local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- Post-16 education and training providers
- Youth support services
- Careers advisers

Once a pupil reaches the age of 16, they can object to any information beyond their name, address and date of birth, being passed to a local authority or provider of youth support services by informing us.

For more information about services for young people, please visit our local authority website.

Local Authorities

We may be required to share information about our pupils with a local authority to ensure that they can conduct their statutory duties including but not necessarily limited to:

- Duties under the Schools Admission and Appeal Codes, including conducting Fair Access Panels
- Reporting children missing in education
- Reporting and managing suspensions and exclusions
- Working with the Virtual Head of School in relation to the education and care of looked after children and, where necessary, previously looked after children
- Reporting and managing safeguarding concerns

Department for Education

The DfE collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the DfE either directly or via a local authority for the purpose of those data collections, under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

School Policies & Procedures

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework. For more information, please see 'How Government uses your data' section below. And for privacy information on the data the DfE collects and uses, please see https://www.gov.uk/government/publications/privacy-information-early-years-foundation-stage-to-key-stage-3 and https://www.gov.uk/government/publications/privacy-information-key-stage-4-and-5-and-adult-education

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 numbers 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)

Data collection requirements

To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to:

https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The data in the NPD is provided as part of the operation of the education system and is used for research and statistical purposes to improve, and promote, the education and well-being of children in England.

The evidence and data provide DfE, education providers, Parliament and the wider public with a clear picture of how the education and children's services sectors are working in order to better target, and evaluate, policy interventions to help ensure all children are kept safe from harm and receive the best possible education.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-npd-privacy-notice/national-pupil-database-npd-privacy-notice

Sharing by the Department

The DfE will only share pupils' data where it is lawful, secure and ethical to do so. Where these conditions are met, 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

School Policies & Procedures

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.

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 UK GDPR, 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 or https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

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

Requesting access to your personal data

The UK GDPR gives parents and pupils certain rights about how their information is collected and used. To make a request for your personal information, or be given access to your child's educational record, contact the Bursar at the School's address.

You also have the right to:

- Be informed about the collection and use of your personal data – this is called the 'right to be informed'
- Ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request, data subject access request or right of access request
- Ask us to change any information you think is not accurate or complete – this is called 'right to rectification'
- Ask us to delete your personal information – this is called 'right to erasure'
- Ask us to stop using your information – this is called 'right to restriction of processing'
- Object to processing' of your information, in certain circumstances
- Withdraw consent at any time (where relevant)

You also have rights in relation to automated decision making and profiling and to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. Examples of some rights not applying include the following:

- Right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- Right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.

School Policies & Procedures

- Right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

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

For further information on how to request access to personal information held centrally by the DfE, please refer back to the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a compliant

Where we are processing your personal data on the basis of consent, you have the right to withdraw that consent. If you change your mind or are unhappy with the use of your personal data, please let us know by contacting the Bursar.

Contact

If you would like to discuss anything in this privacy notice, please contact the Bursar.

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated September 2024.

Appendix C

Privacy Notice

How we use Governors' information

Old Swinford Hospital is the Data Controller for the use of personal data in this privacy notice

The categories of information that we process include

- Personal information such as name, address, date of birth, nationality, country of birth and maiden or former names.
- Confirmation of eligibility to be a governor and in particular, any disqualifications
- Governor appointment dates, term of office and appointing body
- Positions of responsibility for the Governing Body
- Identifying documents such as passport numbers, dates of moving home etc., where necessary
- Skills, experience and qualifications
- Business interests
- Connected persons & interests
- Contact details such as telephone numbers and email addresses
- Disability and access requirements
- Training records
- Attendance
- Minutes and notes of meetings
- Enhanced DBS certification
- References
- Vehicle details for those who use the School's car parking facilities
- Photographs & other visual imagery
- CCTV images
- Site/building access information

Why we collect and use this information

We collect and use this data to:

- Establish eligibility to hold governorship
- Comply with terms of appointment and of office under the Constitution regulations
- Meet the requirements of the Department for Education (DfE)
- Register appointments on the DfE's governor database (GIAS[6])
- Register appointments with the Local Authority
- Maintain a Register of Governors and a register of business and other interests
- Comply with school requirements for safeguarding and security checks
- Inform training needs
- Communicate with you
- Administer Governors' meetings and business
- Record Governance details for example, on the School's website, including attendance, appointing body and roles of responsibility

[6] Get information about schools

- Enter into contracts on behalf of the School
- Establish identity where a person has to do so relevant to their role e.g. to enable the School's Bank to conform to anti-money laundering regulations
- Inform and help make provision for 'reasonable' adjustment where medical conditions, or disabilities, and other reasons make it necessary for these to be considered
- Inform future recruitment
- To comply with insurance disclosure
- Support site and personal security

The lawful basis on which we collect and process this information under UK GDPR

In order to manage and facilitate the governance role, to comply with its obligations and duties to meet the purposes of a school and to safeguard its pupils, the School may process a range of personal data about Governors.

Information is required in the first instance for the purposes of recruitment and verification of eligibility to act as a governor and the School will therefore have a legitimate interest for collecting and processing basic personal data and sensitive personal data.

Thereafter the information we collect and process will be in order to:

- Fulfil its duties and obligations under regulation such as the statutory guidance 'The constitution of governing bodies of maintained schools, 2017' (lawful basis: legal obligation)
- Ensure the safeguarding of pupils (lawful basis: vital interest)
- Effectively and efficiently manage the business of the school (lawful basis; legitimate interest)
- Meet the statutory requirements to provide information to local authorities, the DfE, HMRC and other relevant authorities such as pensions agencies and the School's insurers and, for example, any information required to obtain DBS certification (lawful basis: legal obligation)
- Ensure and sustain the wellbeing and safety of, and promote the development of, governors (lawful basis; legitimate interest)
- Ensure statutory needs of both the school and its governors, such as equality, are met (lawful basis: legal obligation)

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interest of another, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

Collecting information

Most of the information we collect comes from the time when you became a Governor and anything which has been updated since then. Governance roles data is essential for a school's operational use and whilst a great deal of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with UK GDPR, we will inform you whether you are required to provide certain information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing information

We will only collect and retain information for specific purposes and keep it only as long as we need.

Records generated solely for legitimate reasons whilst you are acting as a governor will be disposed of when you leave unless we assess, at that time, that they are required for longer by law or regulation or for other legitimate reasons however we hold some governor and associated role related

information in perpetuity, for example where they form part of the School's permanent records such as the minutes of its meetings.

In respect of any matters of safeguarding information will be kept as long as we require.

Who we share information with and why

We do not share information about individuals in governance roles with anyone without consent unless the law and our policies allow us to do so. We will share information where we are required to do so by law or by order of the court or to prosecuting authorities for the sole purpose of investigations and/or proceedings.

Where we share information we do so only to the extent that it is required for that purpose. We are routinely required to share elements of this information with:

- The DfE
- Ofsted
- Other organisations with whom the School does business or enters agreements such as banks, fund managers, insurers and solicitors for example
- The School's Foundation

We may be required to share collective information via a Freedom of Information request but we will do this only as long as individuals cannot be identified.

We will share safeguarding information where necessary and we will do this in an appropriate way.

Local Authority
We only share information you chose to share so that you may access governor services support and training and receive briefings. Sharing this information provides for an efficient way of accessing training and support services.

Department for Education
The DfE collects personal data from educational settings and further to section 538 of the Education Act 1996, governing bodies are required to provide the Secretary of State with whatever information is required for the purpose of exercising the Secretary of States functions in relation to education. This means that governing bodies must provide to the Secretary of State for Education certain details they hold, as volunteered by their governors, through GIAS and keep the information up to date. Governors are advised that this section of the Act does not require governors to supply information to the governing body. Governors are also informed that information is collected on a voluntary basis but the governing body is required to share what it holds with the Secretary of State for Education. All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework. For more information, please see the 'How Government uses your data' section below.

Others
We also share some of this information with insurers and other service providers such as banks but only to the extent that it is required to provide cover for the school in respect of its business, activities or its workforce or to the extent that it is required to facilitate the business of the School and for the performance of your duties.

We will share information where we are required to do so by law or by order of the court or to prosecuting authorities for the sole purpose of investigations and/or proceedings. Governors are reminded that the School is under duties imposed by law and statutory guidance to record and report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are

proven, where they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO[7] or police.

How Government uses your data

The governance data that we lawfully share with the DfE through GIAS:

- Will increase transparency of governance arrangements
- Will enable maintained schools and academy trusts and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than once context
- Allows the department to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role

Data collection requirements
To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to:

https://www.gov.uk/government/news/national-database-of-governors

Note however that some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to authorised Department for Education (DfE) and education establishment users with a Department for Education (DfE) Sign-in (DSI) account who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless the law allows it.

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 or
https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights

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

Requesting access to your personal data

The UK GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact the Clerk to the Governing Body at Old Swinford Hospital.

You also have the right to:

[7] Local Authority Designated Officer

4If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data on the basis of consent, you have the right to withdraw that consent. If you change your mind or are unhappy with the use of your personal data, please let us know by contacting the Clerk to the Governing Body.

Contact

If you would like to discuss anything in this privacy notice, please contact the Clerk to the Governing Body.

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated September 2024.

Publication Scheme on Information available under the Freedom of Information Act

1. Introduction

1.1. One of the aims of the Freedom of Information Act 2000) is to encourage public authorities, including maintained schools, to be clear and proactive about the information they will make public.

1.2. The School has adopted without modification the model publication scheme of the Information Commissioner's Office.

2. Legislative Framework

2.1. This Policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000 (FOI)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

2.2. It also has regard to the ICO guidance; 'Model publication scheme' 2016 and 'Duty to provide advice and assistance (section 16)' 2016.

3. Principles

3.1. This publication scheme sets out how the School to make information available to the public as part of its normal business activities.

3.2. The publication scheme encourages the School to:-

- Proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the School and falls within the classes of information below.
- Specify the information which is held by the School and falls within the classifications below.
- Proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- Produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- Review and update on a regular basis the information the School makes available under this scheme.
- Produce a schedule of any fees for access to information which is made proactively available.
- Make this publication scheme available to the public.

3.3. If an individual is requesting their personal data that the School holds, then the request will be dealt with as a subject access request (SAR) under article 15 of the GDPR and not under this Policy. Information on how to do this is set out in the School's Records Management & Information Security Policy (see Appendix F).

4. Classes of Information

4.1. In accordance with ICO guidance[8] the following classes of information will be made available:

- **Who we are and what we do**
  Organisational information, locations and contacts, constitutional and legal governance.
- **What we spend and how we spend it**
  Financial information relating to a projected and actual income and expenditure, tendering, procurement and contacts.
- **What our priorities are and how we are doing**
  Strategy and performance information, plans, assessments, inspections and reviews.
- **How we make decisions**
  Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.
- **Our policies and procedures**
  Current written protocols for delivering our functions and responsibilities.
- **Lists and Registers**
  Information held in registers required by law and other lists and registers relating to the functions of the Governors.
- **The services we offer**
  Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

4.2. The School's website (www.oshsch.com) is informative in meeting the needs of publishing information under the publication scheme. The drop down menu bar on the home screen is laid out simply and clearly, guiding the user to matters related to both the curriculum and to boarding, as well as telling users more about the School in general and about its governance.

4.3. Routinely the website hosts information about the daily schedules that make up the school cycle and the range of activities that go on during that cycle. It also provides accessible links to other sources. This information includes:

- Who we are, where we are, and what we do.
- Telling you how to contact us and giving email links for the best person to be in touch with where this is possible.
- Setting out the routes for admission, how to apply and links to the online application system.
- Setting out term dates and the format of the school day as well as the school calendar.
- Detailing curriculum choices at each stage of a pupil's school life.
- Letting you know what it's like to board and what it costs.
- Listing options for extra-curricular activities.
- Showing the governance structure and the basis and terms of appointment.
- Publishing a range of the School's policies, documents and reports.
- Providing copy reports and electronic links to Ofsted inspection outcomes.
- Tabling statistics for academic results and giving links to DfE tables.
- Publishing the latest news, newsletters and the Headmaster's blog.

4.4. Whilst a lot of information will be routinely available on the School's website or accessible through it, such as by accessing links to DfE tables for example, there may be other information where it is

8 'Model publication Scheme' and 'Definition document for the governing bodies of maintained and other state-funded schools in England'

impracticable to publish and maintain in this way. Similarly, not all individuals will wish to access information electronically and in these cases, you can request information be contacting the School using the details below:[9]

Email: lgreen@oshsch.com

Telephone: 01384 817302

Contact address: The Bursar, Old Swinford Hospital, Stourbridge, West Midlands, DY8 1QX.

4.5. In exceptional circumstances some information may be available only by viewing in person. Where this is the case an appointment to view the information can be arranged through the contact details set out above.

4.6. Information will be provided in the language in which it is held or in such other language that is legally required. Where the School is legally required to translate any information it will do so.

4.7. We will take into account our obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats when providing information in accordance with this scheme as far as is reasonable and practicable.

5. Information not Generally Available

The School generally expect to make information in this publication scheme available unless:-

- They do not hold the information
- Disclosure of the information is prevented by law, or is exempt under FOI or is otherwise properly considered to be protected from disclosure
- The information is in draft form
- The information is no longer readily available as it is contained in files that have been placed in archive storage, out of date or otherwise inaccessible

6. Charges for Information Published under this Scheme

6.1. Charges made by the School for routinely published material will be justified and transparent and kept to a minimum. Material which is published and accessed through the website will be provided free of charge.

6.2. Charges may be made for actual disbursements incurred such as photocopying, postage and packaging and the costs directly incurred as a result of viewing information including where hard copies of information freely available on the website are required.

6.3. The School does not have to comply with any FOI request that exceeds the statutorily imposed appropriate limit of £450.

6.4. When determining whether the cost of complying with an FOI request is within the appropriate limit, the School will take account only of the costs we reasonably expect to incur in relation to:

- Determining whether it holds the information
- Locating and retrieving the information, or a document which may contain the information
- Extracting the information from a document containing it
- Costs related to the time spent by any person undertaking any of the activities in this search, or in communicating with the individual

6.5. Where multiple requests for information are made within 60 consecutive working days of each other, either by a single person or by different persons who appear to be acting in concert, the

[9] Response to FOI requests will only be made by the Bursar or, where delegated, through the DPO. Any staff receiving FOI requests should redirect the request to the Bursar

estimated cost of complying with any of the requests will be taken to be the total costs to the School of complying with all of them.

6.6. Charges may also be made for information provided under this scheme where they are legally authorised, they are in all circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published scheme or scheduled of fees which is readily available to the public.

6.7. If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

6.8. When calculating the 20th working day in which to respond to a request, the period beginning the day on which the fee notice is given to the applicant and ending with the day on which the fee is received, will be disregarded.

7. Requests for Information not Published Under this Scheme

Information held by a public authority that is not published under this scheme can be requested in writing. Its provision will be considered in accordance with the provisions of the Freedom of Information Act.

8. How to Request Information

8.1. To help us process your request please clearly mark any request or correspondence PUBLICATION SCHEME REQUEST.

8.2. Your request must state the name of the applicant, email and telephone contact details and an address for correspondence and it must clearly describe the information you are asking for.

8.3. Provided that the request is complete the School will endeavour respond no later than 20 school days from receipt of the request. In doing this the School with confirm or deny to the person making a request for information to the School either holds, or does not hold, information of the description specified in the request and, if it does it will provide the relevant documentation always provided that the information is of a type which is not prohibited from distribution. If there will be a delay in responding to the enquiry the School will write and explain why this is and what timeframe they reasonably expect to be able to respond in.

8.4. The School will not provide information where:

- They reasonably require further information to meet an FOI request, has informed the applicant of this requirement, but was not subsequently supplied with that further information
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons
- A request for information is exempt under section 2 of the Freedom of Information Act 2000
- The information would identify another individual and disclosure would be in breach of data protection regulations
- The cost of providing the information exceeds the appropriate limit
- The request is vexatious
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one
- A fee notice was not honoured

8.5. Where information is, or is thought to be, exempt, the School will, within 20 school days, give notice to the applicant which states that fact and specifies the relevant exemption.

9. Providing Advice and Assistance

9.1. The School will meet its duty to provide advice and assistance, as far as is reasonable, to any person who proposes to make, or has made, requests for information to the School.

9.2. They will provide assistance for each individual on a case-by-case basis and may offer advice and assistance in the following circumstances for example:

- If an individual requests to know what types of information the School holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
- If a request has been made, but the School is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
- If a request has been refused, e.g. due to an excessive cost, and it is necessary for the School to assist the individual who has submitted the request.
- If an individual is unsure of their rights under the Freedom of Information Act 2000
- Advising an applicant if information is available elsewhere and how to access this information or if the information is to be published at a later date.

9.3. If an applicant decides not to follow the School's advice and assistance and fails to provide clarification, the School is under no obligation to contact the applicant again.

10. Policy Revision

This Policy is generally reviewed annually but may be reviewed at other times to ensure compliance with current legislation and is therefore subject to change without prior notice.

CCTV Policy

1. Introduction

1.1. The School takes its responsibility towards the safety of pupils, staff, visitors and its site very seriously and to assist in this use surveillance cameras to monitor the site and its entrances and exits.

1.2. The purpose of this Policy is to manage and regulate the use of the surveillance and CCTV systems at the school which capture images of people who could be identified and thereby ensure that:

- We comply with obligations under data protection regulation.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

2. Legislative Framework

2.1. This Policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000 (FOI)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2. It also has regard to ICO guidance ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

3. Principles

3.1. What is our system for

The School is committed to enhancing the quality of life on campus by integrating the best practices of campus safety with state of the art technology. A critical component of a comprehensive security program is the use of CCTV. We use CCTV in various locations, all public areas, around the school site. CCTV information will only be used for the safety and security of the school and its staff, pupils and visitors and for law enforcement purposes.

CCTV monitoring is used to assist in protecting the School community and property by acting as a deterrent for criminal and other inappropriate behaviours and for damage to the school. It is limited to uses that do not violate the reasonable expectation of privacy as defined by the law and monitoring will be conducted in a manner consistent with the existing school policies and with particular reference to GDPR.

Information obtained by CCTV monitoring will only be released when authorised by the Headmaster or the Bursar.

School Policies & Procedures

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.

3.2. Who is responsible for our CCTV system

The School, as the corporate body, is the data controller. The Governing Body therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

Operationally CCTV will be the responsibility of the Bursar and any enquiries about the CCTV system should therefore be directed to the Bursar.

3.3. Clear policies and procedures

A code of practice has been established to ensure that sufficient and proper arrangements in place for the operation of CCTV.

3.4. Review of the use of CCTV

New developments in the law and industry standards and protections will be periodically reviewed.

3.5. Image retention

Images and related data collected by CCTV are the property of Old Swinford Hospital.

Secure storage and measures to protect data will be put in place. Recordings will not be stored beyond the agreed period unless authorised and for a specific purpose.

4. Definitions

4.1. In accordance with the surveillance code of conduct:

- 'Surveillance' is the monitoring the movements and behaviour of individuals; this can include video, audio or live footage.
- Overt surveillance is the use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- Covert surveillance is the use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

4.2. The School does not generally use covert surveillance. It will be instigated only in extreme circumstances by the authority of the Headmaster.

4.3. Any overt surveillance footage will be clearly signposted around the school.

5. CCTV Code of Practice

5.1. The purpose of this code of practice is to regulate the use of CCTV to monitor and record on campus for the purposes of safety and security.

5.2. This code of practice applies to all personnel and property of the School in the use of CCTV monitoring and recording.

5.3. The School will:

- Have a rationale for introducing monitoring in a location.
- Process surveillance and CCTV footage legally and fairly.
- Collect surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collect surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensure that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.

- Protect footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

5.4. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

- The Headmaster, Bursar, Senior Duty Team, ICT Manager and Site Manager have the authority to view all CCTV recordings for the safety and security purposes at the School.
- The Headmaster and Bursar are authorised to oversee and coordinate the use of CCTV monitoring equipment at the School.

5.5. The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

5.6. The surveillance system has been designed for maximum effectiveness and efficiency however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

5.7. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

5.8. The Bursar will monitor new developments in the law and industry standards and protections.

5.9. Appropriate signage will be in place on the School site.

5.10. The camera viewing positions will be limited so that there will be no view of residential housing off campus.

5.11. Data storage, security and deletion:

- CCTV recorded data will be held on a separate hard drive for each building. The hard drive and monitor is password protected to prevent tampering or duplication of the information.
- Recordings will be stored for a period not exceeding 31 days and will be automatically erased by the recording equipment. Images can be stored by the Headmaster or Bursar to storage devices if required for further use.
- Disc media that is required to be stored (for police purposes) will be stored in a secure location with access authorised by the Headmaster or Bursar.

5.12. Mobile or portable CCTV equipment may be used after approval by the Headmaster or Bursar to ensure the safety and security of the School community.

5.13. The DPO will ensure that surveillance and CCTV footage is handled and processed in accordance with data protection legislation and that it is obtained and subsequently destroyed in line with legal requirements.

5.14. The ICO's Checklist for users of limited CCTV systems monitoring small retails and business premises will be reviewed on an annual basis by the Bursar

6. Access

6.1. Under GDPR, individuals have the right to obtain confirmation that their personal information is being processed. Individuals have the right to submit a Subject Access Request to gain access to their personal data in order to verify the lawfulness of the processing. Information on how to do this is set out in the School's Records Management & Information Security Policy (see Appendix F).

6.2. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headmaster, who will consult the DPO, on a case-by-case basis, with close regard to data protection and freedom of information legislation and particularly where innocent/unrelated third parties may be identified as part of the footage.

6.3. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

6.4. All disks containing images belong to, and remain the property of, the School.

7. Site/Buildings Access monitoring

7.1. The School has an access security system which records entry and exit from the site and in and out of buildings and rooms within some buildings. The purpose of this is to support the safety and security of individuals. It is used to control access to the school site and to identify the location of individuals, for example but not limited to, accounting for people in the event of evacuation or lockdown (including drills), or where there is concern for a missing child or for any safeguarding issue.

7.2. Site/buildings access security is a recent introduction. Access to records of movements onto/off the school site and in to/out of rooms and buildings is restricted to the Bursar. The Headmaster can authorise access if the Bursar is not available. Records will be maintained for a period of three years. The retention policy will be revisited as part of the ongoing policy review process to determine if the period is sufficient or insufficient.

8. Policy Revision

This Policy is generally reviewed annually but may be reviewed at other times to ensure compliance with current legislation and is therefore subject to change without prior notice.

Records Management & Information Security Policy

1. Introduction

1.1. The School recognises that by efficiently managing its records, it will be better able to comply with its legal and regulatory obligations and contribute to the effective overall management of the school. Records provide evidence for protecting the legal rights and interests of the School and provide evidence for demonstrating performance and accountability.

1.2. The School is also committed to maintaining the confidentiality of its information and ensuring that records are only accessible by the appropriate persons.

1.3. This Policy provides the framework through which effective and proper management can be achieved.

1.4. It has been drawn up within the context of the GDPR Data Protection Policy and its related appendices and with reference to the DfE's advice 'Data protection: a toolkit for schools (2018)'.

2. Scope of the Policy

2.1. The Policy applies to all records created, received or maintained by staff or volunteers of the School in the course of carrying out its functions.

2.2. Records are defined as all those documents which facilitate the business carried out by the School and which are thereafter retained, or retained for a set period, to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

3. Responsibilities

3.1. The School has a responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this Policy, and its implementation is the Headmaster however data security is a whole school matter and everyone's responsibility.

3.2. The DPO is responsible for records management in the School and for promoting and monitoring compliance with policy. The DPO is responsible for ensuring that all records are securely stored and appropriately disposed of at the end of the relevant period.

3.3. Individual staff and volunteers are responsible for ensuring that records for which they are responsible are accurate, maintained securely and disposed of correctly, in line with the provisions of this Policy.

4. Retention

4.1. There is no sector wide retention policy that prescribes how long all categories of data should be retained for. The School therefore looks to best practice together with considering the needs of the school and the context in which the information might be required. The School refers to the Information Records Management Society (IRMS) and the DfE for its principal sources of guidance.

4.2. Retention depends upon the purpose data was collected for and any subsequent events or incidences that may impact upon the retention period, for example, safeguarding matters arising. The focus should be on the time period that is 'necessary and proportionate'.

4.3. A small percentage of the School's records may be selected for permanent preservation as part of the School's archives and for historical research.

5. Storing and Protecting Information

General

5.1. It is the School's aim that:

- Information is protected against unauthorized access
- Confidentiality of information is assured
- Integrity of information is maintained
- Regulatory and legislative requirements are met.

5.2. It aims to do this through applying standards and procedures which will include:

- Acceptable use policies
- Data storage and backup procedures
- Asset identification and control
- Physical and environmental security
- Developing and maintaining secure processing systems

5.3. It is the responsibility of each member of staff to adhere to policy, standards and procedures.

5.4. All confidential records will have restricted access and appropriate safe storage.

5.5. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information.

5.6. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information should be supervised at all times.

5.7. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with GDPR, either in an electronic or paper form, staff must take extra care to follow the same procedures for security, e.g. keeping devices secure and ensuring that no information is copied to or left accessible on any computer which has general use or cannot be adequately secured. The person taking the information from the school premises has full responsibility for the security of the data.

5.8. Before sharing data, staff will ensure that:

- They have consent from individuals to share it
- Adequate security is in place to protect it
- The data recipient has been outlined in a privacy notice

Paper based information

5.9. Confidential paper records will be kept in a locked storage with restricted access.

5.10. They must not be left unattended or in clear view when held in a location with general access or in the presence of unauthorised personnel.

Digital based information

5.11. Devices holding personal data or data applications must have appropriate security programmes running to protect them from viruses and potential hacking.

5.12. Terminals and applications will have appropriate access restrictions and must not be left in accessible mode or visually displaying confidential information in a location with general access or in the presence of unauthorised personnel. School and/or personal laptops and similar devises must not be used to hold any School personal and/or sensitive data

5.13. Staff are provided with their own secure login and password for systems relevant to their role and, or, position. There are protocols for safe use of electronic devices and for construction and managing passwords.[10]

5.14. Digital personal data should be coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up and where personal data is saved on removable storage or a portable device, the device will be encrypted and kept in appropriate safe storage when not in use.

6. Accessing Information

6.1. All members of staff, parents of registered pupils and other users of the School and its facilities have the right to access certain personal data being held about them or their child. 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

6.2. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

6.3. Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

6.4. 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.

6.5. 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.

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

7. How to Request Information

7.1. To help us process your request please clearly mark any request or correspondence SUBJECT ACCESS REQUEST. You can send this to the Bursar whose details are set out at the end of this Policy:[11]

[10] E-Mail, Internet, Tablet & Mobile Phone Policy for Employees and Password Policy for Employees

[11] Response to SAR requests will be coordinated and made by the Bursar or, where delegated, through the DPO. Any staff receiving SAR requests should redirect the request to the Bursar

7.2. In exceptional circumstances some information may be available only by viewing in person. Where this is the case an appointment to view the information can be arranged through the contact details already set out above.

7.3. Your request must state the name of the applicant, email and telephone contact details and an address for correspondence and it must clearly describe the information you are asking for.

7.4. 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

7.5. 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

7.6. If such an application is made the School will verify the identity of the person making the request before any information is supplied. When this has been confirmed a copy of the information will be supplied to the individual free of charge.12

7.7. All requests will be responded to without delay and within one month of receipt.

7.8. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

7.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

7.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. When a request is refused, the School will tell the individual why and tell them they have the right to complain to the ICO.

8. Exercising Other Data Protection Rights of the Individual

8.1. In addition to the right to make a subject access request as outlined above and to receive information when their data is collected about how it will be used and processed, data protection law gives individuals rights to, for example:

- Ask for the rectification of any inaccurate or incomplete personal data.
- Object and prevent their personal data being used for direct marketing.
- Challenge processing which has been justified on the basis of legitimate interests or the performance of a task in the public interest.
- Object to decisions based solely on automated decision making or profiling.
- Have their data erased where there is no compelling reason for its continued processing.
- Restrict the processing of their data in certain circumstances such as where the data is inaccurate for example.

[12] The School may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

- Ask for their personal data to be transferred to a third party so that the individual can obtain and reuse their personal data for their own purposes across different services.
- Withdraw their consent to processing at any time.

8.2. To help us process your request please clearly mark any request or correspondence DATA PROTECTION RIGHTS. You can send this to the Bursar whose details are set out at the end of this Policy:[13]

8.3. Where the request is for rectification and the personal data in question has been disclosed to third parties, the School will inform them of the rectification where possible and inform the individual about the third parties that the data has been disclosed to.

8.4. The School will also inform relevant third parties with whom data has been shared in the event of erasure or restrictions on processing, subject to this being possible and not involving disproportionate effort to do so.

8.5. Requests will generally be responded to within one month; this will be extended by two months where the request is complex or a number of requests have been received and in this case the individual will be notified of this and the reason for the extension.

8.6. There may be circumstances in which the individuals request cannot be carried out, for example, where the School has a right to refuse in certain circumstances or where the personal data concerns more than one individual and providing the information would prejudice the rights of any other individual. Where a request is refused the School will tell the individual why and tell them they have the right to complain to the ICO.

9. Information Audit

9.1. The DPO will, from time to time, conduct information audits to evaluate the information the School is holding, receiving and using, and to ensure that this is correctly managed in accordance with GDPR. This may take the form of interviews with staff members and or questionnaires as well as general visits around site.

9.2. The DPO will assess from these audits the School's ongoing data needs, the information needed to meet those needs, appropriateness of storage formats, retention periods and protective marking.

9.3. Audits will include ensuring that surveillance and CCTV footage is handled and processed in accordance with the CCTV Code of Practice and data protection legislation.

10. Marking and Disposal of Information

10.1. Information needs to be appropriately marked to identify its degree of confidentiality however all personal data has some degree of confidentiality. It will therefore be the protocol in this school to assume data will not be routinely marked unless it is either restricted or confidential.

10.2. 'Restricted' will be used to identify data or information that can identify an individual person or child and places that person or child at risk of harm. It also applies to information which is sensitive data or when for example group summaries are prepared on a personal characteristic or data set such as SEN. Restricted by definition implies restricted circulation i.e. on a need to know basis only.

10.3. 'Confidential' applies to highly sensitive information or data, including commercially sensitive information, where unauthorised disclosure, even within the School, is not permitted or may put someone's personal safety at high risk.

10.4. Where data or information should be 'reviewed prior to disposal' it should be marked as such so as to ensure it is retained as the circumstances at that time then indicate.

[13] Response to requests under other data protection rights will be coordinated and made by the Bursar or, where delegated, through the DPO. Any staff receiving such a request should redirect the request to the Bursar

10.5. Non-sensitive information can be disposed of in ordinary rubbish or recycling bins. It is unlikely that any document containing personal data will fall into this category.

10.6. Any information which contains personal data or is specifically categorised either restricted or confidential should be disposed of in the containers designated for such waste and which are emptied under agreed protocol. Where we use a third party to safely dispose of records on the School's behalf they will be required to provide sufficient guarantees that they comply with data protection law.

10.7. Personal data should only be kept in a form which permits the identification of individuals for no longer than is necessary for the purposes for which the personal data are processed. The DPO will ensure that data (both in paper and digital form) is reviewed annually. [14]

10.8. Where files or data are marked as 'to be reviewed before disposal' the relevant member of staff will do this in liaison with the DPO.

10.9. Where information must be kept permanently it is exempt from the normal review procedures

11. Policy Revision

This Policy is generally reviewed annually but may be reviewed at other times to ensure compliance with current legislation and is therefore subject to change without prior notice.

Contact Details for the Bursar for enquiries referred to in the Policy

Email: lgreen@oshsch.com

Telephone: 01384 817302

Contact address: The Bursar, Old Swinford Hospital, Stourbridge, West Midlands, DY8 1QX

[14] Review and disposal may be arranged for quieter time of the year and therefore disposal may not be on the exact calculated date for each individual item. The School consider this a reasonable approach to adopt.