Yesodey Hatorah Senior Girls School

Data protection policy and Freedom of Information policy

Approved by:	Finance and Resources Committee	**Date:**	June 2025
Last reviewed on:	May 2025		
Next review due by:	May 2026		

Contents

Data Protection Policy

1. Introduction

This policy sets out process and procedures for Yesodey Hatorah Senior Girls School meeting their GDPR legal obligations to anyone involved with the school or any of its activities.

2. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK Data Protection Law.

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

3. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

4. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental health
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. The data controller

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

The school is registered with the ICO, as legally required.

6. Roles and responsibilities

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

6.1 Governing board

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

6.2 Data protection officer

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

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

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

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

Our DPO is Shard Business Services, and is contactable via dpo@shardbusinessservices.co.uk.

Our DP Lead is Mrs A Glick and is contactable via YHS on 0208 826 5500.

6.3 Headteacher

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

6.4 All staff

Staff are responsible for:

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

7. Data protection principles

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

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

8. Collecting personal data

8.1 Lawfulness, fairness, and transparency

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

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

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

8.2 Limitation, minimisation, and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

9. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

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

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

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

Where we transfer personal data internationally, we will do so in accordance with data protection la

10. Subject access requests and other rights of individuals

10.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

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

10.2 Children and subject access requests

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

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

10.3 Responding to subject access requests

When responding to requests, we:

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

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.4 Access to School Records

In line with the school's commitment to minimising non-essential site attendance, and taking into account site security requirements and operational resource constraints, requests for access to school information or records — including, without limitation, the inspection of meeting minutes — will ordinarily be fulfilled by the provision of digital copies.

Requests will be actioned as soon as practicable and within one calendar month following receipt. However, some documents may contain third party personal data or sensitive information that requires review and, where appropriate, redaction. Where this is the case, the requester will be advised of any expected delay and kept updated on progress.

Physical inspection of records on site will only be accommodated where necessary and where it can be safely accommodated.

10.5 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

11. Parental requests to see the educational record

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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12. Biometric recognition systems

At present, Yesodey Hatorah Senior Girls School does not collect, possess or use biometric data relating to its pupils or staff.

Should the school's policy in relation to biometric information change, the School would act in accordance with the Government's advice and relevant legislation.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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

Any enquiries about the CCTV system should be directed to the Headteacher.

14. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 14 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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

Consent can be refused or withdrawn at any time. If consent is withdrawn, from that point onwards, we do not continue to store or share publicly any photos or videos with that pupil.

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.

15. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Yesodey Hatorah Senior Girls School recognises that AI poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Yesodey Hatorah Senior Girls School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

16. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

17. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety and acceptable use policy and agreements)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

18. Disposal of records

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

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

19. Personal data breaches

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

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

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

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

20. Training

All staff and governors are provided with data protection training as part of their induction process. Staff will also be informed of their responsibility to the legislation.

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

21. Freedom of Information Requests

Closely linked to GDPR regulations is the Freedom of Information Act 2000, which requires all public authorities to adopt and maintain a publication scheme. To see the publication scheme and more information, please see the end of this policy.

Freedom of Information requests must be submitted in writing, including email. Requests will be responded to within 20 school days or 60 working days, whichever is shorter. We endeavour to share the information as soon as it is collated in line with the principle of openness. If we do not hold the information requested, we will inform the requester. If you wish to request access to your/your child's personal data, please see the section on subject access requests.

Please note, there are some exemptions to the FOI Act 2000, most commonly the 'public interest test' which means we will evaluate the public interest of the information being shared. We will do this whilst maintaining a commitment to openness and scrutiny. Repeated or vexatious claims will be refused. We can also refuse requests if the cost / manpower required to deal with the request is too large. The limit of cost incurred is £450; the ICO state schools should rate staff time at £25 per person per hour, which allows for 18 staff hours.

For any further information, please contact our DPO.

21.1 Access to School Records

In line with the school's commitment to minimising non-essential site attendance, and taking into account site security requirements and operational resource constraints, requests for access to school information or records — including, without limitation, the inspection of meeting minutes — will ordinarily be fulfilled by the provision of digital copies.

Requests will be actioned as soon as practicable and within 20 school days following receipt. However, some documents may contain personal data or commercially sensitive information that requires review and, where appropriate, redaction. Where this is the case, the requester will be advised of any expected delay and kept updated on progress.

Physical inspection of records on site will only be accommodated where necessary and where it can be safely accommodated.

22. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full Governing Body.

23. Links with other policies

This data protection policy is linked to our:

- Child Protection Policy
- Online Safety policy and acceptable use agreements
- Freedom of information publication scheme
- Privacy Notice

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email and/or phone, confirming the information has been noted.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

› The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

› The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in a file in the DPO's office. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

› The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of an example of a data breach if it was to occur, focusing especially on breaches involving particularly risky or sensitive information. Other examples would lead to an equivalent response. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

› If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

› Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

› If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

› In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

› The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

› The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

› If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform the local authority.

Appendix 2: Freedom of Information Publication Scheme

Introduction

The Freedom of Information Act 2000 applies to Yesodey Hatorah Senior Girls' School. This publication scheme commits the school to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the school.

The school has adapted the Model Publication Scheme that has been prepared and approved by the Information Commissioners Office (ICO).

The scheme commits 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 classifications below.
- To specify the information that is held by the school and falls within the classifications below.
- To 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.
- To review and update, on a regular basis, the information the school makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.

Classes of Information

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 projected and actual income and expenditure, tendering, procurement, and contracts.

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 function of the school.

The service we offer

Advice and guidance, booklets and leaflets and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure
- Information in draft form
- Information that 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.
- The method by which information published under this scheme will be made available
- The school will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of the school, information will be provided on our school website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, the school will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

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.

Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. 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 on a website will be provided free of charge.

Charges may be made for information, subject to a charging regime specified by parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packing
- the costs directly incurred because of viewing information

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

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 the provision of the information.

Written Requests

Information held by the school that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act. We will respond to Freedom of Information Acts within 20 school days or 60 working days, whichever is shorter.

Contact Details

If you require a paper version of any information, or want to ask whether information is available, please contact the school reception by telephone, email, or letter. Contact details are set out below or you can visit the school website.

Website: https://www.yesodeyhatorah.org

Tel: 020 8826 5500

Email: admin@yesodeyhatorah.org

Address: 6 Egerton Road, N16 6UA

To help us process requests quickly, any correspondence should be clearly marked “PUBLICATION SCHEME REQUEST”.

Guide to information available from the school under the Model Publication Scheme

Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 1 – Who we are and what we do **Organisational information, structures, locations, and contacts** **This will be current information only**		
Who is in the school	Website	Free of charge
Who is who on the Governing Body and the basis of their appointment	Website	Free of charge

Instrument of Government	Hard copy	Schedule of charges
Contact details for the Headteachers and for the Chair of Governors (named contacts where possible with telephone number and Email address (if used))	Website	Free of charge
School prospectus	Website	Free of charge
Annual Review	Website	Free of charge
Staffing structure	Hard copy	Schedule of charges
School sessions times and term dates	Website	No charge
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 2 – What we spend and how we spend it **Financial information relating to projected and actual income and expenditure, procurement, contracts, and financial audit** **Current and previous financial year as a minimum**		
Annual budget plan and financial statements	Hard copy	Schedule of charges
Capitalised funding	Hard copy	Schedule of charges
Additional funding	Hard copy	Schedule of charges
Procurement and projects	Hard copy	Schedule of charges
Pay policy	Hard copy	Schedule of charges
Staffing and grading structure	Hard copy	Schedule of charges
Governor's allowances	Hard copy	Schedule of charges
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 3 – what our priorities are and how we are doing **Strategies and plans, performance indicators, auditors, audits, inspections, and reviews** **Current information as a minimum**		
School profile Government supplied performance data The latest Ofsted report – Summary and Full Report	Hard copy Website	Schedule of charges Free of charge
Performance Management policy and procedures adopted by the Governing Body	Hard copy	Schedule of charges
School Improvement Plan	Hard copy	Schedule of charges
Safeguarding policies and procedures	Website	Free of charge
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 4 – How we make decisions		

Decision making processes and records of decisions Current and previous three years as a minimum		
Admissions Policy/decisions (not individual admission decisions)	Website	Free of charge
Agendas of meetings of the governing body and (if held) its sub-committees	Hard copy	Schedule of charges
Minutes of meeting (as above) – NB this will exclude information that is properly regarded as private to the meetings	Hard copy	Schedule of charges
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 5 – Our policies and procedures **Current written protocols, policies, and procedures for delivering our services and responsibilities** **Current information only**		
School policies including: Charging and remissions policy Health and Safety Staff conduct policy Discipline and grievance policies Equality and diversity (including equal opportunities) policies Staff recruitment policies	 Website Website Website Website Website Website Website	 Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge
Pupil and curriculum policies, including: Home-school agreement Curriculum Sex education Special education needs Accessibility Race equality Collective worship Careers education Pupil discipline	 Website Website Website Website Website Website Website Website Website	 Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge Free of charge
Records management and personal data policies, including: Information security policies Records retention Data protection policies	 Website Website Website	 Free of charge Free of charge Free of charge
Charging regimes and policies This should include details of any statutory charging regimes. Charging policies should include charges made for information routinely published. They should clearly state what costs are to be recovered, the basis on which they are made and how they are calculated.	Website	Free of charge
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 6 – Lists and registers **Currently maintained lists and registers only**		
Curriculum circulars and statutory instruments	Hard copy	Schedule of charges

Disclosure logs	Hard copy	Schedule of charges
Asset register	Hard copy	Schedule of charges
Any information the school is currently legally required to hold in publicly available registers THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER	Hard copy	Schedule of charges
Information to be published	How the information can be obtained (hard copy and/or website)	Cost
Class 7 – The service we offer **Information about the service we offer, including leaflets, guidance and newsletters produced for the public and businesses** **Current information only**		
Extra-curricular activities	Website	Free of charge
Out of school clubs	Website	Free of charge
School publications	Website	Free of charge
Services for which the school is entitled to recover a fee, together with those fees	Website	Free of charge
Leaflets books and newsletters	Website	Free of charge
Additional information This will provide the school with the opportunity to publish information that is not itemised in the lists above		

Schedule of Charges

This describes how the charges have been arrived at and should be published as part of the guide

Type of charge	Description	Basis of charge
Disbursement costs	Photocopying/printing @ 10p per A4 sheet (black and white)	Actual cost
	Photocopying/printing @ 30p per sheet A4 (colour)	Actual cost
	Postage	Actual cost of Royal Mail standard 2nd class
Statutory Fee		In accordance with relevant legislation