GIRLINGTON PRIMARY SCHOOL

Data Protection

General Data Protection Regulation (GDPR) Policy

Date Policy Written:	Spring 2026
Date Policy Ratified:	Spring 2026
Date Policy to be Reviewed:	Spring 2027

GIRLINGTON PRIMARY SCHOOL	Reviewed By
(Statutory) S4 **Data Protection - General Data Protection Regulation (GDPR) Policy** *Appendix 1 – Privacy notices* *Appendix 2 – GDPR Quick information sheet* *Appendix 3 – CCTV Schools security policy* *Appendix 4 – Freedom of Information*	SBM_____ DH_____

Contents

1. Aims

We aim 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 data protection legislation (the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

This policy meets the requirements of the UK GDPR following the incorporation of the EU GDPR into UK legislation, with some amendments outlined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data (if any). It also reflects the ICO's code of practice 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.

3. 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.
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 • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. 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.

4. The data controller

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

The school is registered with the Information Commissioner's Office (ICO) and shall pay the appropriate registration fee annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer

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

The DPO may be asked to 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 first point of contact for individuals whose data the school processes is the school business manager/office. However, individuals may contact the DPO direct. The DPO is first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in the Service Level Agreement.

Our DPO is Ben Cain – Fusion Business Solutions Limited – dpo@feps.co.uk - Tel 01924 907319

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - 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

6. 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
- Accountability

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

The school maintains a Record of Processing Activities (ROPA) as required by Article 30 UK GDPR. This records all processing including:

- **Pupil data**: Name, UPN, attendance, attainment (MIS: Arbor/SIMS), SEN/behaviour (CPOMS), photos/videos, biometrics (meals). Lawful basis: public task (Education Acts). Recipients: DfE, LA, safeguarding partners. Retention: IRMS Toolkit.
- **Staff data**: HR records, DBS, payroll. Lawful basis: contract/legal obligation. Recipients: pension providers, HMRC.
- **Parent data**: Contacts, permissions. Lawful basis: legitimate interests/public task.
  The full ROPA is available from the DPO and reviewed annually."
- **Governor data:** Contact details, terms of office, roles and responsibilities, attendance records, declarations of interest, training records, and where applicable DBS checks. Lawful basis: public task and legal obligation. Recipients: Local Authority, DfE (e.g. Get Information About Schools), and governance support services. Retention: IRMS Toolkit.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

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

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

Whilst the majority of digital systems we use in school are to support the teaching and learning of our pupils, and therefore we have a legal basis for processing, there may be times that we use other tools. Where we offer such online services to pupils and we intend to rely on consent as a

basis for processing, we will get parental consent (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. We will take appropriate steps to ensure that the data held is accurate such as regular data verification exercises.

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in line with the record of processing activities and the retention schedule as detailed in the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent if this is appropriate 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 data sharing agreement where significant amounts of personal data or special category data is being shared with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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 including to the European Economic Area, we will do so in accordance with UK data protection law.

We appoint processors only after due diligence. Key processors and Data Processing Agreements (DPAs) include:

- Arbor/SIMS (MIS): DPA ensures UK hosting, encryption, sub-processor approval.

- CPOMS (safeguarding): DPA covers access logs, breach notification <72hrs.
- Evolve/ParentPay (trips/payments): DPA mandates pseudonymisation where possible. All DPAs require Article 28 compliance: security, audits, confidentiality. List updated in ROPA.

For transfers outside UK (e.g., Microsoft 365 if non-UK servers), we use:

- International Data Transfer Agreements (IDTAs) with EU adequacy supplement for EEA.
- For others: safeguards per ICO Transfer Risk Assessment Tool.
  No unrestricted transfers; all assessed for Schrems II compliance. Details in ROPA.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

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

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

If staff receive a subject access request they must immediately notify their line manager and the DPO.

9.2 Children and subject access requests

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

Children below the age of 12 are generally not 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 be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we cannot 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 forecast, 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 in order to cover our administration costs.

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

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

9.4 Other data protection rights of the individual

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

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

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

10. Parental requests to see the educational record

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. This right applies up to the child's 18th birthday.

11. Biometric recognition systems

Pupils

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

If we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

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

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Staff

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

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

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

Any enquiries about the CCTV system should be directed to the Site Manager/School Business Manager.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We have a legal basis for doing so for the purpose of identifying pupils. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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 how the photograph and/or video will be used.

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

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

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

Parents/students will not be permitted to take photographs or make videos other than for their own personal and domestic use. Such photographs and videos will not be shared publicly – e.g. via social media.

14. 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 privacy 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
- Putting appropriate checks in place if we transfer any personal data outside the UK where no adequacy agreements are in place
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

A Data Protection Impact Assessment (DPIA) will be conducted for high-risk processing per ICO guidance, including:

- Biometric systems (e.g., fingerprint meals).
- CCTV deployment.
- New edtech/AI tools processing pupil data.
  The DPO leads DPIAs using ICO template, consulting affected parties and governing board if risks remain high post-mitigation. Completed DPIAs are stored securely and reviewed before launch.
    -

15. 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
- Passwords should be 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 to change their passwords at regular intervals and 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.
- 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)

16. 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.

17. Personal data breaches

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

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

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

- 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

18. Training

All staff are provided with data protection training as part of their induction process. In line with the ICO recommendation, refresher training will be provided to all staff regularly.

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every year** in accordance with Department for Education's advice on statutory policies and will presented to the full governing board for approval.

20. Links with other policies

This data protection policy is linked to our: **Please only refer to the policies you have in place**

- Freedom of information policy
- Staff code of conduct
- Acceptable use of ICT/Digital technology
- Safeguarding and Child Protection

Appendix 1

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the data protection lead person in the school/organisation, who will contact the DPO.

1. The DPO will assist in the investigation of 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
2. The DPO will determine whether to alert the Head Teacher/Chair of Governors.
3. The DPO will assist in making all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
4. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
5. The DPO will determine whether the breach meets the threshold to be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms using the ICO's self-assessment tool.
6. The DPO will ensure that the decision is documented (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system, or on a designated software solution.
7. Where the ICO must be notified, the DPO will do this by telephone or via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO

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

8. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
9. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact and ensure that any decision on whether to contact individuals is documented. If the risk is high, the DPO, or data protection lead will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out in plain language:
    - 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
10. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
11. The data protection lead person in School, with advice and/or support from 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 on the school's computer system, or on a designated software solution.

- In the case of a significant breach, the DPO, headteacher or designated senior leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the data protection lead person as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the data protection lead will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the data protection lead will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- Written confirmation that the email has been deleted will be requested from all the individuals who received the data, confirming that they have complied with this request
- In the case of a serious breach, we will arrange for an internet search to be conducted 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

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

GIRLINGTON PRIMARY SCHOOL

Girlington Road, Bradford, West Yorkshire, BD8 9NR
Headteacher: Mrs Kathryn Swales
Telephone: 01274 493543 Fax: 01274 543874

Privacy Notice (How we use pupil information)

Data Protection Legislation

In accordance with UK data protection law individuals have the right to know what personal data we hold about them, and for what purpose.

This Privacy Notice explains how we collect, use, store and share personal data about pupils and their parents/carers. In data protection law, these activities are called data processing.

The categories of personal data we may process include:

- Personal information (such as name, unique pupil number and address, identification documents)
- Parental/carer contact information (name, telephone number, home address and email address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information and results of internal and externally set tests
- Relevant medical information
- Special Educational Needs information
- Exclusions / behavioural information

Certain information is deemed to be "special category" which is more sensitive personal data. This includes, but is not restricted to,

- information about any medical conditions, including physical and mental health;
- photographs and CCTV footage captured in school

Why we collect and use this information

We use the pupil and parent/carer data listed above:

To support pupil learning
To keep children safe
To monitor and report on pupil progress
To provide appropriate pastoral care
To assess the quality of our services
To comply with the law regarding data sharing

To assist with our administration and communication systems – for example, text messaging and cashless services in school.

The lawful basis on which we hold this information

We collect and use pupil and parent/carer information in accordance with the Information Commissioners' Office (ICO) guidance on the lawful basis for processing as indicated below:

- Processing is necessary for compliance with a legal obligation. For instance, in order to comply with the legislation such as:
  - Education Act 1996 and 2002;
  - The Education (Pupil Information) (England) Regulations 2005;
  - Keeping Children Safe in Education regulations (updated annually).

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- Explicit consent has been given

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. For safeguarding purposes, we will need to collect contact information from parents and have a legitimate interest to share this information, on occasion, with all parties who have designated parental responsibility to verify its accuracy.

Storing pupil data

We hold pupil data in line with the Information Records Management Society Toolkit for Schools (see www.IRMS.org.uk / toolkit for schools)

Who we share pupil information with

We routinely share pupil information with:

- Schools or colleges that pupils attend after leaving us
- Local authorities
- The Department for Education (DfE) and other government departments
- Health services (NHS/Public Health England)
- Police forces, courts, tribunals
- Educational IT system providers such as SIMS, CPOMs, assessment tracking, Tapestry, Class Dojo, Timestables Rockstars

Why we share pupil information

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013.

Data collection requirements:

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

The National Pupil Database (NPD)

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

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

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

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

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the **Headteacher / Data Protection Officer.**

Parents or those with parent responsibility have the right to access their child's educational record. This right applies as long as the pupil is aged under 18.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

Complaints

We take complaints about our processing of personal data very seriously. If you believe our processing of your personal data or that of your child is unfair, misleading or inappropriate or have any other concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/ telephone 0303 123 1113, or write to: ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Contact us

If you would like to discuss anything in this privacy notice, please contact:

Ben Cain – Data Protection Officer
Email: Ben@fusionbusiness.org.uk

Commented [BC1]: Update to DPO@feps.co.uk

GIRLINGTON PRIMARY SCHOOL

Girlington Road, Bradford, West Yorkshire, BD8 9NR
Headteacher: Mrs Kathryn Swales
Telephone: 01274 493543 Fax: 01274 543874

Privacy Notice (How we use school workforce information)

Data Protection Legislation

In accordance with UK data protection law individuals have the right to know what personal data we hold about them, and for what purpose.

This Privacy Notice explains how we collect, use, store and share personal data about members of staff. In data protection law, these activities are called data processing.

The categories of school workforce information that we collect, process, hold and share include (not exhaustive):

- Personal information (such as name, employee or teacher number, national insurance number, home address, personal telephone contact details and next of kin/emergency contact)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Relevant medical and disability information
- Contract information (such as start dates, hours worked, post, roles, salary and pension information)
- Work absence information (such as number of absences and reasons such as sickness and maternity, adoption and paternity leave)
- Qualifications (and, where relevant, subjects taught)
- Discipline, grievance, performance management, monitoring of teaching standards and absence management information
- Evidence of the right to work in the UK
- Signing in/out register
- Images on CCTV
- Involvement in school trips.

Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid
- To meet the requirements of the Keeping Children Safe in Education regulations and safeguarding our pupils
- To contact staff and other nominated persons in the event of an emergency or unforeseen urgent circumstance.

- To enable school to provide access to school systems – e.g. SIMS and educational tools
- Defense of legal claims
- To comply with the Department for Education regulations
- To plan and monitor expenditure on staff salaries within the school's budget
- To comply with legislation in relation to data sharing

The lawful basis on which we process this information

School collects and processes this information under the powers given to schools and local authorities for the legitimate interests of the controller or third party, where applicable.

The following categories of lawfulness apply:

- Processing is necessary for the performance of an employment contract with the data subject or to take steps to enter into a contract
- Processing is necessary in order to comply with the law
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for carrying out our obligations under employment, social security or social protection law, or a collective agreement.
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems

An example of a legal obligation for data collection purposes (Departmental Censuses) is the Education Act 1996 – this information can be found in the guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools

In the rare circumstances that we cannot rely on a specified legal basis to process your information, we will obtain your explicit consent before doing so.

Collecting this information

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 data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold our school workforce data in line with the Information Records Management Society. http://irms.org.uk.

Who we share this information with

We routinely share this information with:

- Our local authority
- The Department for Education (DfE)
- The school's insurance company
- Payroll and personnel administration service
- Human Resources service
- Our text messenger service

- Other software providers, so that you can carry out your duties, for example CPOMS, Evolve etc. local authority staff development platform (Leeds For Learning/Skills for Bradford)

We will share your information with third parties with whom the school enters into a contract for the delivery of services such as payroll and occupational health.

Why we share school workforce information

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

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

Data collection requirements

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

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

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

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

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

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

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

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

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, in the first instance contact the **Headteacher or the data protection lead in school. Alternatively, you can contact the Data Protection Officer.**

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

Complaints

We take complaints about our processing of personal data very seriously. If you believe our processing of your personal data or that of your child is unfair, misleading or inappropriate or have any other concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/ telephone 0303 123 1113, or write to: ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Contact us

If you would like to discuss anything in this privacy notice, please contact:

Ben Cain – Data Protection Officer

Email: Ben@fusionbusiness.org.uk

Commented [BC2]: Update to DPO@feps.co.uk

GIRLINGTON PRIMARY SCHOOL

Girlington Road, Bradford, West Yorkshire, BD8 9NR
Headteacher: Mrs Kathryn Swales
Telephone: 01274 493543 Fax: 01274 543874

Privacy Notice (How we use volunteer workforce information)

Data Protection Legislation

In accordance with UK data protection law individuals have the right to know what personal data we hold about them, and for what purpose.

This Privacy Notice explains how we collect, use, store and share personal data about volunteers which includes school governors and associate members. In data protection law, these activities are called data processing.

The categories of volunteer workforce information that we collect, process, hold and share include (not exhaustive):

- Personal information (such as name, employee or teacher number, national insurance number, home address, personal telephone contact details and next of kin/emergency contact)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Relevant medical and disability information
- Qualifications (and, where relevant, subjects taught)
- Signing in/out register
- Images on CCTV
- Involvement in school trips.

Why we collect and use this information

We use school volunteer workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- To meet the requirements of the Keeping Children Safe in Education regulations and safeguarding our pupils
- To contact you or your nominated person in the event of an emergency or unforeseen urgent circumstance.
- Defense of legal claims
- To comply with legislation in relation to data sharing

The lawful basis on which we process this information

School collects and processes this information under the powers given to schools and local authorities for the legitimate interests of the controller or third party, where applicable.

The following categories of lawfulness apply:

- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for carrying out obligation under employment, social security or social protection law, or a collective agreement.
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

In the rare circumstances that we cannot rely on a specific legal basis to process your information, we will obtain your explicit consent before doing so.

Collecting this information

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 data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school volunteer workforce data in line with the Information Records Management Society. http://irms.org.uk.

Who we share this information with

We routinely share this information with:

- Our local authority
- The Department for Education (DfE)
- The school's insurance company
- Human Resources service
- Our text messenger service
- Other software providers, so that you can carry out your duties, for example CPOMS, Evolve, local authority platform (Leeds For Learning/Skills for Bradford)

We will share your information with third parties with whom the school enters into a contract for the delivery of services such as governor support service, educational resource providers.

Why we share school volunteer workforce information

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, in the first instance contact the Head Teacher / Data protection lead in school. Alternatively you can contact the Data Protection Officer.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means

- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

Complaints

We take complaints about our processing of personal data very seriously. If you believe our processing of your personal data or that of your child is unfair, misleading or inappropriate or have any other concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/ telephone 0303 123 1113, or write to: ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Contact us

If you would like to discuss anything in this privacy notice, please contact:

Ben Cain – Data Protection Officer

Email: Ben@fusionbusiness.org.uk

Commented [BC3]: Update to DPO@feps.co.uk

GIRLINGTON PRIMARY SCHOOL

Girlington Road, Bradford, West Yorkshire, BD8 9NR
Headteacher: Mrs Kathryn Swales
Telephone: 01274 493543 Fax: 01274 543874

Privacy Notice for Job Applicants

The school is registered with the information Commissioners Office (ICO) under the provisions of the UK General Data Protection Regulation (GDPR) and Data Protection Act. The school takes its responsibilities under the GDPR very seriously. This notice provides details of how we collect and uses information about you.

What is this information?

We may collect some or all of the following information about you as part of our recruitment process:

- Name, address and contact details
- Application data and application history
- Education and employment details
- Gender, ethnicity, disability, sexual orientation and religion/belief
- Date of birth and national insurance number, Identification, Immigration and Asylum details, i.e. right to work in the UK
- References if you are invited to interview
- Right to work in the UK and supporting documentation if you are invited to interview
- Copies of qualifications if you are invited to interview

Who uses this information?

People involved in the recruitment process for example, School Business Manager, Headteacher and Governors.

What authority do we have to collect and use this information?

Under the GDPR we collect and use this information under powers given to schools for the legitimate interests of the controller or third party, where applicable.

The following categories of lawfulness apply:

- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

In rare circumstances where no legal authority exists to use your information, we will obtain your express consent first.

What is 'personally identifiable data' (PII)?

The term PII relates to any data that could potentially identify a living person. The following fields in Human Resources are classified as PII: name, age, address, place of birth, date of birth, gender, national insurance number, any application data and any information about an individual that can be used directly, or in connection with other data, to identify, contact or locate that person.

Why do we use this information?

We use this information in the course of recruiting members of staff.

Who are we likely to share this information with?

We may sometimes share the information we have collected about you where it is necessary, lawful and fair to do so. In each case we will only share the minimum amount of information, only when required, for the following reasons:

With the local authority and our HR services provider to allow managers to manage recruitment processes.

How do we keep this information secure?

Your information is stored securely on database and document management systems with stringent limited access. All access to documents is limited to only those staff involved within the recruitment process.

How long do we keep this information?

Documents are kept for a period of 6 months following the end of the recruitment process. If you are successfully appointed into a post, your data will be held in line with school policies. A copy of the staff privacy notice will be provided to you upon appointment with full details.

What are your rights?

You have the right to request that we stop processing your personal data. Wherever possible, we will seek to comply with your request but we may need to hold or process information in connection with one or more of the school's legal functions.

If you have any questions about our use of this data, or you wish to request a copy of the information we hold about you, or you wish to discuss your rights in relation to opting out from these processes, please contact our **Data Protection Officer, Ben Cain** who can be contacted by email at Ben@fusionbusiness.org.uk

Commented [BC4]: Update to DPO@feps.co.uk

Appendix 2

GDPR Staff Quick Information Sheet – How to Keep Personal Data Safe

Personal data: any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information

Sensitive personal data: includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals

DO:

- ✓ **Remember that data protection laws DO NOT stop you from reporting safeguarding concerns**
  - You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this
- ✓ **Only collect the information you actually need**
  - When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
  - If you don't need it, or only want it "Just in case", don't collect it
  - If you've already collected personal information that you don't need, delete it
- ✓ **Keep personal data anonymous, if possible**
  - For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to
  - This is particularly important with photographs for external use – if you have an image of a child, don't attach their name to it unless you have explicit consent to do so
- ✓ **Think before you put information up on the wall**
  - If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments**. Still only display the information you really need to display.**
  - If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it
- ✓ **Take care if you are required to take personal information home with you**
  - Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
  - Store the documents in a safe place at home – don't leave them in your car or at a friend's house
  - Best practice to access the school network from home or use your encrypted USB stick.
- ✓ **Practise good ICT security**
  - Passwords should be at least 8 characters, with upper and lower-case letters and special characters

- Password-protect documents and email attachments that include personal data. Preferably use Galexkey or Egress Switch (free secure email service).
- Always double-check that you're emailing personal data to the correct person, who is authorised to see it
- Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers
- Do not use personal laptops for school use.
- Do not use your personal email account for any school business
- Do not send personal information by Fax or email (Egress switch is a free secure email service).
- Do not share your user ID/password with anyone.
- Keep your Apple ID secure and remember it as this will be required at a later date.,
- Keep your iPad up to date with the latest security updates, keep a secure pincode.
- Do not log in with your user ID for anyone, all staff have their own User ID/password.
- Do not share the school WIFI password with anyone, visitors to use "gpguest"
- Supply teachers are given their own username and password but are limited on the school network (access to scratchpad, printing, software installed on the computer and the internet).
- Do not leave your computer unlocked/logged in when unattended (certain staff members have access to secure drives which contain confidential data).
  To lock your computer hold down the windows key and press L.
- If you are required to take personal data home, do not leave the information unattended.
- When working on confidential files ensure your computer screen cannot be viewed by unauthorised personnel.
- Do not allow family/friends access to school equipment (laptops).
- All USB sticks **must be** encrypted with bitlocker, please see Balal for help with this.
- If your laptop or iPad is lost/stolen please report this to Kathryn, Diana Parker and Balal ASAP.
- For more information refer to the Girlington's "Acceptable Use Policy – Staff and Volunteers" available in the Staffbook drive.
- Remember – at all times treat people's personal information as you would wish your own to be treated.

DON'T:

× **Leave personal data out on your desk**

- Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen

× **Take any sensitive personal information home with you**

- If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place

If something doesn't seem right, talk to the School Business Manager (SBM).

Report to our SBM immediately if you think personal data has been lost, stolen or wrongly disclosed. This is so we can quickly take steps to mitigate the impact of the breach.

You should also speak to our SBM

- You have any concerns at all about keeping personal data safe
- You're introducing a new process or policy that involves using personal data
- Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information

The SBM will work closely with our DPO (Data Protection Officer) regarding GDPR

Appendix 3

CCTV Schools Security Policy.

1. Introduction

1.1 Girlington Primary School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

1.2 The system comprises of 16 cameras.

1.3 The CCTV system is owned and operated by the school.

1.4 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

1.5 The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the Act.

1.6 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

2. Statement of Intent

2.1 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

http://www.ico.org.uk/1542/cctv-code-of-practice-pdf

2.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the school, including school gates if coverage includes outdoor areas. In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.3 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas. Where a camera may overlook an area outside of the school i.e a public road, neighbouring property, a sufficient privacy assessment will be undertaken to ensure the capture of images does not interfere with the publics rights and freedoms.

3.3 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. Covert Monitoring

4.1 The school may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from a member of the senior management team.

4.3 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

5. Storage and Retention of CCTV images

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely.

6. Access to CCTV images

6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and Data Protection Act.

7.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within 1 calendar month of receiving the request .

7.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 Requests should be made in writing to the Governing Body.

8.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018

Appendix A - Checklist

This CCTV system and the images produced by it are controlled by Girlington Primary School who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 2018).

Girlington Primary School has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of stakeholders. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Staff and members of the school community will be consulted about the proposal to install CCTV equipment.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix B – CCTV Signage

It is a requirement of the Data Protection Act 2018 and supporting guidance to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries

Commented [BC5]: Not required as the principles set out in the GDPR policy cover what is required within this element of the documentation. Advise to remove Appendix C entirely as no longer required.

- site or computer system, where there are security measures and processes in place

If something doesn't seem right, talk to the School Business Manager (SBM).

Report to our SBM immediately if you think personal data has been lost, stolen or wrongly disclosed. This is so we can quickly take steps to mitigate the impact of the breach.

You should also speak to our SBM

- You have any concerns at all about keeping personal data safe
- You're introducing a new process or policy that involves using personal data
- Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information

The SBM will work closely with our DPO (Data Protection Officer) regarding GDPR

Appendix D

Freedom of Information

Background

The Freedom of Information Act 2000 (FOIA) is legislation that requires schools to publish certain categories of information and entitles the general public to access other information held by our school (subject to certain exceptions) within an agreed timeframe. This policy applies to all information held by school regardless of how it was created or received, the method of recording (ie electronic, paper) or the age of the information. It includes information still held in draft format. A notable exception to this entitlement is personal information such as student and staff records, which is covered by the Data Protection Act 2018 and the school's data protection policy. If the data requested falls into this category, school may redact, or refuse to supply the information.

Publication Scheme
One of the aims of the FOIA is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

To do this the school produces a publication scheme, setting out:

- The classes of information that it publishes or intends to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment.

The scheme covers information already published and information which is to be published in the future. Some information that the school holds will not be made public, for example personal information. Wherever possible, the school will seek to publish this information on the school website at www.girlingtonprimary.co.uk

Maintained schools must publish certain information online. This is regularly updated by the DfE at https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

The classes of information that the school undertakes to make available are organised into four broad topic areas:

School Website	information published on the school website.
Governors' Documents	information relating to Governors and Governors Meetings and in other governing body documents.
Pupils and Curriculum	information about policies that relate to pupils and the school curriculum.
School Policies	information about policies that relate to the school in general.

Further information is contained with Appendix A. Single copies of information covered by this publication will be provided free unless stated otherwise. If a parental request means that the school has a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications or videos the school will let the parent know the cost before fulfilling the request.

Dealing with Requests

All requests under the FOIA will be dealt with promptly, within the statutory timescale of no more than 20 working days. If, in exceptional circumstances, this cannot be met, we will write to the individual concerned with an explanation and a proposed timescale.

There is no requirement for requests to mention the FOIA and all requests in writing will be treated as FOIA requests. If the information falls within an area exempted within the FOIA, school will advise of this and offer assistance (such as offering such generic information as can be provided)

If there are repeated and vexatious requests for information, school will seek further advice and reserves the right to refuse to provide the information under such circumstances. In addition, school may refuse requests where the statutory maximum cost of provision (currently £450) would be exceeded. In these cases we would expect to enter a dialogue with the requester to reduce the scope and range of the request so some information can be provided.

Information will be provided free of charge but postage will be charged for if appropriate and applicable.

Checklist for action on receipt of a request for information

- Decide whether the request is a request under DPA, EIR or FOI
- Decide whether the school holds the information or whether the request should be transferred to another body if the information is held by them
- Provide the information if it has already been made public
- Inform the enquirer if the information is not held
- Consider whether a third party's interests might be affected by disclosure and if so consult them
- Consider whether any exemptions apply and whether they are absolute or qualified
- Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information
- Decide whether the estimated cost of complying with the request will exceed the limit of £500.
- If a request is made for a document that contains exempt personal information ensure that the personal information is removed by applying the redaction procedure
- Consider whether the request is vexatious or repeated

Further provisions of FOIA Schools are under a duty to provide advice and assistance to anyone requesting information.

The enquirer is entitled to be told whether the school holds the information (the duty to confirm or deny) except where certain exemptions apply.

A well managed records and management information system is essential to help schools to meet requests.

Requests should be dealt with within 20 days excluding school holidays.

Wilfully concealing, damaging or destroying information in order to avoid answering an enquiry is an offence. A valid FOI request should be in writing, state the enquirer's name and correspondence address and describe the information requested.

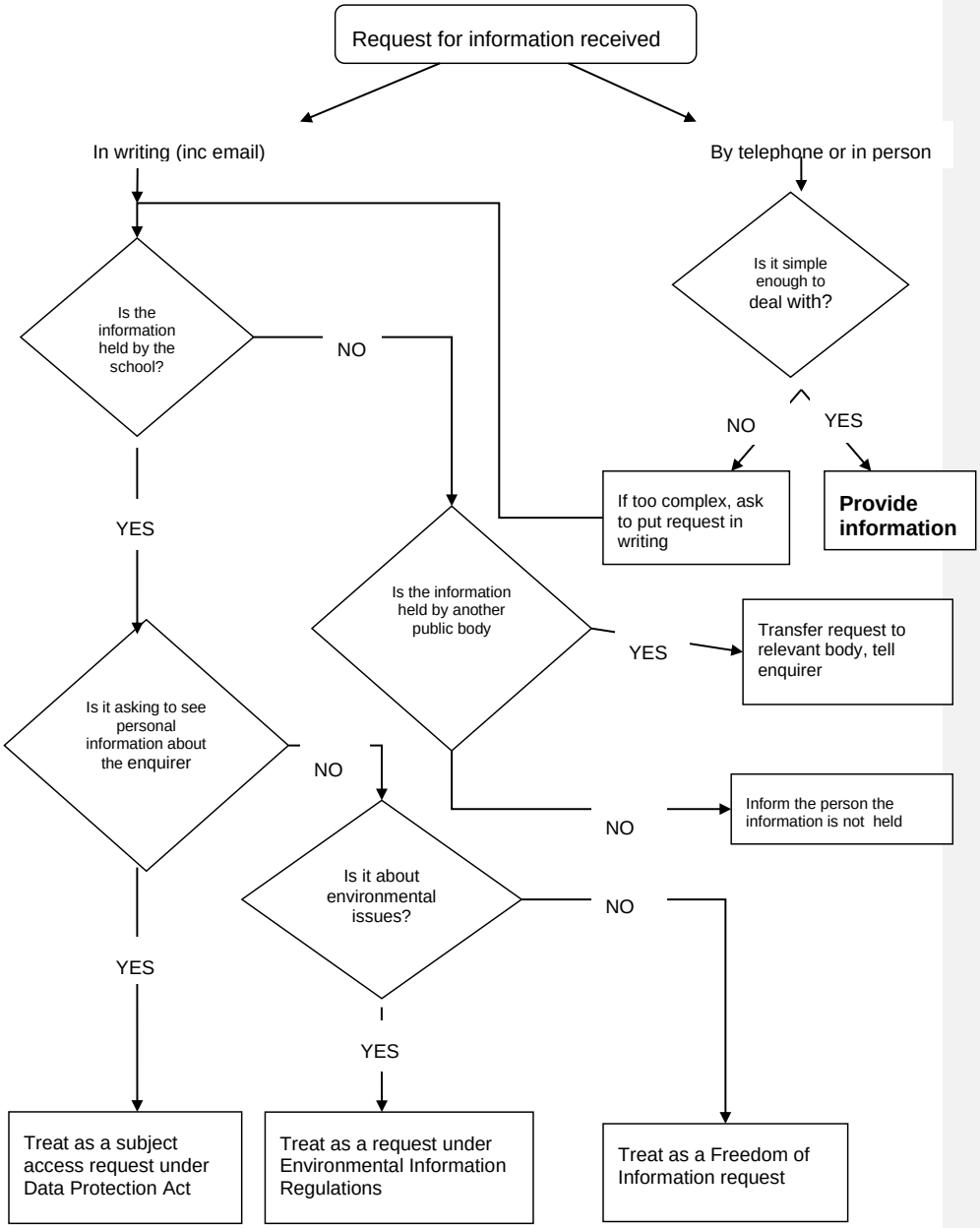
Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

Exemptions and classes of information

Third Party Information
Consideration will be given to requests for third party information such as staff or personal data to avoid breaches of confidence and breaches of the Data Protection Act. In these circumstances, information will be withheld. This relates to any data related to a living individual classed as 'personal data' under the Data Protection Act 2018. If an individual can be identified when names are redacted, this information must be withheld.

Contractual information
The school may withhold contractual information relating to suppliers if it could be treated as a breach of confidence. Any consideration of the release of information must be discussed with the relevant organisation, along with consideration of the FOIA exceptions which cover commercial confidentiality, such as FOIA Awareness Guide No 5. The school will consider each request in line with the regulations.

Flow diagram for responding to a request for information



Appendix A - Classes of Information Currently Published

School Website – this section sets out information published on the school website.

Class	Description
School Prospectus (on school website)	The statutory contents of the school prospectus are as follows, (other items may be included in the prospectus at the school's discretion): • the name, address and telephone number of the school, and the type of school • the names of the Headteacher and Chair of Governors • information on the school policy on admissions • the Ofsted report • a statement of the school's ethos and values • details of any affiliations with a particular religion or religious denomination, the religious education provided, parents' right to withdraw their child from religious education and collective worship and the alternative provision for those pupils • information about the school's policy on providing for pupils with special educational needs • information about the school's Pupil Premium policy and outcomes • information about the use of the PE and Sport premium • number of pupils on roll and rates of pupils' authorised and unauthorised absences • National Curriculum assessment results for appropriate Key Stages, with national summary figures • the curriculum • the arrangements for visits to the school by prospective parents

Information relating to the governing body– this section sets out information published in the Governors' Annual Report and in other governing body documents.

Class	Description
Governors' Information	Details of the structure and responsibilities of the Governing Body and it's committees Information about each Governor, including: • full name • date of appointment • term of office • business and financial interests • Who appointed them • Governance roles in other educational institutions • Material relationships between Governors and School Staff • Attendance record at GB and committee meetings over the last academic year
Instrument of Government	• The name of the school • The category of the school • The name of the governing body • The manner in which the governing body is constituted • The term of office of each category of governor if less than 4 years • The name of any body entitled to appoint any category of governor • Details of any trust • If the school has a religious character, a description of the ethos • The date the instrument takes effect
Minutes [1] of meeting of the governing body and its committees	Visit reports from each Governing Body meeting and access arrangements for minutes from specific meetings and sub committee meetings.

[1] Some information might be confidential or otherwise exempt from the publication by law – we cannot therefore publish this

Pupils & Curriculum Policies - This section gives access to information about policies that relate to pupils and the school curriculum.

Class	Description
Home – school agreement	Statement of the school's aims and values, the school's responsibilities, the parental responsibilities and the school's expectations of its pupils for example homework arrangements
Curriculum Policy	Statement on following the policy for the secular curriculum subjects and religious education and schemes of work and syllabuses currently used by the school
Sex Education Policy	Statement of policy with regard to sex and relationship education
Special Education Needs Policy	Information about the school's policy on providing for pupils with special educational needs
Accessibility Plans	Plan for increasing participation of disabled pupils in the school's curriculum, improving the accessibility of the physical environment and improving delivery of information to disabled pupils.
Equalities Policy	Statement of policy for promoting equalities
Collective Worship	Statement of arrangements for the required daily act of collective worship
Safeguarding Policy	Statement of policy for safeguarding and promoting welfare of pupils at the school.
Behaviour Policy	Statement of general principles on behaviour and discipline and of measures taken by the head teacher to prevent bullying.

School Policies and other information related to the school - This section gives access to information about policies that relate to the school in general.

Class	Description
Published reports of Ofsted referring expressly to the school	Published report of the last inspection of the school and the summary of the report and where appropriate inspection reports of religious education in those schools designated as having a religious character

Post-Ofsted inspection action plan	A plan setting out the actions required following the last Ofsted inspection and where appropriate an action plan following inspection of religious education where the school is designated as having a religious character
Charging and Remissions Policies	A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example school publications, music tuition, trips
School session times and term dates	Details of school session and dates of school terms and holidays
Health and Safety Policy and risk assessment	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy
Complaints procedure	Statement of procedures for dealing with complaints
Performance Management of Staff	Statement of procedures adopted by the governing body relating to the performance management of staff and the annual report of the head teacher on the effectiveness of appraisal procedures
Staff Conduct, Discipline and Grievance	Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance
Curriculum circulars and statutory instruments	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education and Skills to the head teacher or governing body relating to the curriculum

Single copies are available from school free of charge and all information is contained within the school website.