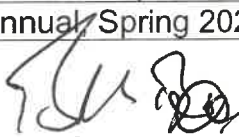


**Green Park School
GDPR (General Data Protection Regulation)
Freedom of Information Statement (FOI)
CCTV (Data Protection)**

Policy written by:	Amy Tura
Role:	Assistant SBM
Committee approving Policy	Resources
Date approved by Committee:	13th February 2023
Date for renewal:	Bi Annual Spring 2025
Signed by Chair of Committee	 Mr B Bond or Rev S Skidmore (delete as appropriate)

Our Mission

Green Park aims to provide access to high quality education and learning experiences, both in school and in the community and seeks to maximise each pupil's achievement as part of his or her lifelong learning. It is the school's aim to be a centre of Educational Excellence in the heart of the community.

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Collecting personal data
8. Sharing personal data
9. Subject access requests and other rights of individuals
10. Parental requests to see the educational record
11. CCTV
12. Photographs and videos
13. Data protection by design and default
14. Data security and storage of records
15. Disposal of records
16. Personal data breaches
17. Training
18. Monitoring arrangements

19. Freedom Of Information (FOI)

Appendix 1: Personal data breach procedure

Appendix 2: Website - Privacy Notice and Data Protection procedure

Appendix 3: Privacy Notice (How we use school workforce information)

Appendix 4: Freedom of Information

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the 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 GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

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	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs

	<ul style="list-style-type: none"> • 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 as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 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.

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 **Services4Schools**. Email: dpo@greenparkschool.co.uk

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - 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 European Economic Area
 - 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 GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

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

- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

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

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

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

On-Line Services and Apps

If we offer online services to all pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, school will r parental consent (except for online counselling and preventive services, where consent from the pupil is also required).

Third Parties do not usually hold personal data of pupils via the Apps used, however staff will always check this is the case with **Eservice technicians** beforehand. For pupils in special schools we will get consent from parents. Whenever we first collect personal data directly from individuals (e.g. the admission form), we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's [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: **(Appendix 2)**

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

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for: **(Appendix 3)**

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

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

Subject access requests should include:

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

If staff receive a subject access request they must immediately forward it to the DPO: **Services4Schools. Email: dpo@greenparkschool.co.uk**

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.

Special Schools - Primary

Children below the age of 12 or in Special Schools 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.

Special Schools - Secondary

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

9.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

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

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

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

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

9.4 Other data protection rights of the individual

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

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

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

10. Parental requests to see the educational record

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.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe.

We will adhere to the ICO's [code of practice](#) for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to **Mrs Lorraine Dawney, Headteacher.**

12. Photographs and videos

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

We will obtain written consent from parents/carers 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.

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

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

Uses may include:

- Within school on notice boards and in school 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.

See our **Child Protection and Safeguarding Policy and Policy for the Use of Camera's and Images** for more information on our use of photographs and videos.

13. Data protection by design and default

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

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

14. Data security and storage of records

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

In particular:

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

15. Disposal of records

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

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

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in **Appendix 1**.

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

- 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

17. Training

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

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

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

19. Freedom Of Information Act

This data protection policy is linked to our:

- Freedom of information publication scheme – See Appendix 4

Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO provider, Services4Schools at dpo@greenparkschool.co.uk
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored [set out where you keep records of these decisions – for example, on the school's computer system, or on a designated software solution]
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored [set out where you will keep these records – for example, on the school's computer system, or on a designated software solution]
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

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

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*
- *Staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*

Appendix 2:



GDPR PRIVACY NOTICE

For Pupils and their Parents of

Green Park School

Who processes your information?

Green Park School is the data controller of the personal information you provide to us. This means the school is responsible for deciding how information you provide us with is used. We refer to your information as “personal data” and when we use your information in different ways, this is called “processing”. The General Data Protection Regulation (GDPR) outlines how personal data should be protected and used appropriately by organisations.

In some cases, your personal data will be shared with other people, organisations or companies. This sharing will only occur after we have sought your permission (consent), unless the law requires us to do so. If we share your personal data outside of school, we ensure that the same data protection standards are upheld by other people involved in processing your personal data.

The categories of pupil information that we process include:

- Personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- Characteristics (such as ethnicity, language, and free school meal eligibility)
- Safeguarding information (such as court orders and professional involvement)
- Images (such as photographs and CCTV images)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment (such as Key Stage 1 and 2 and phonics results)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)

Why do we collect and use your information?

Green Park School holds the right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, local authorities and / or the DfE. We collect and use personal data



in order to meet legal requirements and our public task duties and obligations set out in the GDPR and UK law, including those in relation to the following:

- Education Act 1996
- The Education (Information About Individual Pupils) (England) Regulations 2013
- The Children Act 1989 & 2004

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To keep children safe (food allergies, or emergency contact details)
- To meet the statutory duties placed upon us for DfE data collections

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. The school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

The categories of parent information that the school collects, holds and shares includes the following:

- Contact information, including addresses, phone numbers and email addresses of parents and/or any other emergency contacts
- Financial and meal management information, e.g. account and transactional information for school meals and eligibility for free school meals
- Information pertaining to home life where appropriate, e.g. where a pupil is identified as having a mental health issue or there are safeguarding concerns

How long is your data stored for?

Personal data relating to pupils at Green Park School and their families is stored in line with the school's Data Protection Policy.

In accordance with GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

We will also retain personal data in the form of images, registers and examples of work for the purposes of archiving and as a historical record of school life. This information may later be published in school literature, displays or external media. In this case, the personal data we retain will be proportionate and limited to what is necessary.

Will my information be shared?

The school is required to share pupils' data with the 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 the DfE under regulation 3 of The Education (Information about Individual Pupils) (England) Regulations 2013. The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Green Park School is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NPD with third parties who promote the education or wellbeing of children in England by:

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

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NPD is maintained.

To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

Green Park School does not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. The school routinely shares pupils' information with:

- Pupils' destinations upon leaving the school
- Wolverhampton Council and its agencies (Social Services, SEND Team, LAC Team)
- Other Local Authorities (as needed)
- The NHS and other health professionals (School Nurses)
- The Department for Education
- Other Government agencies (Ofsted)
- External Support Agencies (Welfare support, Inclusion and Behaviour Services)
- The providers of our management information system (Capita SIMS)
- The software we use to communicate with you (Teachers2Parents)
- Our Safeguarding system (CPOMS)
- The system we use for managing visitors to school (Inventory)
- Our virtual learning environment
- The providers of our learning platform (CloudW, E-Services Team)
- The systems we use for recording progress in learning (EFL)
- The online software we use to help deliver the curriculum (EFL, Twinkl)
- The software we use to provide cashless payments (School Money)
- The online software we use to help us manage visit and health & safety (Evolve)
- The providers of therapy and support services (Art Therapy, LA Speech and Language Team and Visually Impaired Team)

- Local Authority Auditors (Wolverhampton LA)
- Visit/trip providers (Kingswood, Swimming / Activity Centres)
- Alternative Education Providers (Squirrel)
- School Photographer (Tempest)
- Professional advisors and consultants (LA School Improvement Team, Teaching Schools)
- Contract Catering Services (Wolverhampton LA Contract Catering)
- Contract Data Management Services (Services4Schools)
- Contract IT Support Services (E-Services)

What are your rights?

Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- Request access to the personal data that Green Park School holds
- 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
- Request that your personal data is amended if it is inaccurate or incomplete
- Request that your personal data is erased where there is no compelling reason for its continued processing

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

Where can you find out more information?

For more information about the Department for Education'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 for Education has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-recvied>

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

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

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 our Data Protection at DPO@greenparkschool.co.uk or by writing to Green Park School, Green Park Avenue, Bilston, WV14 6EH. Please address letters: For the attention of 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
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact

If you would like to discuss anything in this privacy notice, please contact: DPO@greenparkschool.co.uk or by writing to Green Park School, Green Park Avenue, Bilston, WV14 6EH.

Appendix 3: Privacy Notice (How we use school workforce information)

The EU General Data Protection Regulation (GDPR)

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by a new Act giving effect to its provisions. Before that time the DPA will continue to apply.

Data Controller

Green Park School complies with the GDPR and is registered as a 'Data Controller' with the Information Commissioner's Office (Reg. No. Z6331497).

The Data Protection Officer (DPO) for the School is Mr James Plant, from Services4Schools.

We ensure that your personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)

Why we collect and use staff 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

The lawful basis on which we process this information

We process this information under Article 6, and one from Article 9 where data processed is special category data from the GDPR from 25 May 2018.

(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>

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.

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body
- protecting vulnerable individuals;
- the prevention and detection of crime

Storing this information

We hold school workforce data for Green Park School and the local authority for a retention period of **7 years**.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

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.

Local authority

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

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) 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, contact Mrs Lorraine Dawney or Mrs Sam Briscoe (HR Officer/PA to Headteacher).

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

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

Withdrawal of Consent

The lawful basis upon which the School process personal data is that it is necessary in order to comply with the Schools legal obligations and to enable it to perform tasks carried out in the public interest.

Where the School process personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent in writing.

Further information

If you would like to discuss anything in this privacy notice, please contact:
Mrs L Dawney, Headteacher or Email: DPO@greenparkschool.co.uk

Appendix 4 : Freedom Of Information

Contents	Page
Statement of intent	24
Legal framework	24
Accepting requests for information	24
General right of access to information held by the school	25
The appropriate limit	26
Charging fees	27
Means by which communication is to be made	27
Providing advice and assistance	28
Publication scheme	30
Monitoring and review	30
Appendix a) Model Publication Scheme	31

Statement of Intent

Green Park School has an obligation to publish a freedom of information statement, outlining how we will meet our duties under the Freedom of Information Act 2000 and associated regulations. The development and effective implementation of this policy fulfils that requirement.

More specifically, this policy outlines:

- How the School will respond to requests from individuals for access to information held about them.
- Our School's policy and procedures for the release and publication of private data and public records.
- Our School's policy and procedures for providing applicants with advice and assistance throughout the duration of their requests.

It also clarifies our position regarding the appropriate limit to the costs incurred by the school in obtaining any requested information, and on charging fees for its provision.

1. Legal framework

This policy has due regard to the following legislation:

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

This policy also has due regard to guidance, including, but not limited to, the following:

- ICO 'Model publication scheme'

- ICO 'Duty to provide advice and assistance (section 16)'

This policy will be viewed in conjunction with the following other School policies:

- Green Park School Data Protection Policy

2. Accepting requests for information

The School will only accept a request for information which meets all of the following criteria:

- It is in writing.
- It states the name of the applicant and an address for correspondence.
- It describes the information requested.

A request will be treated as made in writing if it meets all of the following requirements:

- It is transmitted by electronic means.
- It is received in legible form.
- It is capable of being used for subsequent reference.

The School will publish details of its procedures for dealing with requests for information on the website, which includes:

- A contact address and email address.
- A telephone number.
- A named individual to assist applicants with their requests.

3. General right of access to information held by the School

Provided that the request complies with section 2 of this policy, the School will, no later than 20 working days from receipt of the request, comply with its duty to:

- Confirm or deny to any person making a request for information to the School, whether it holds information of the description specified in the request.
- Provide the documentation, if the School confirms that it holds the requested information.

The School will not comply with section 3.1 of this policy where:

- The School reasonably requires further information to meet a freedom of information request, has informed the applicant of this requirement, but was not subsequently supplied with that further information.
- The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.
- A request for information is exempt under section 2 of the Freedom of Information Act 2000.
- The cost of providing the information exceeds the appropriate limit.
- The request is vexatious.
- The request is a repeated request from the same person made within 60 consecutive working days of the initial one.
- A fee notice was not honoured.

Where information is, or is thought to be, exempt, the School will, within 20 working days, give notice to the applicant which:

- States the fact.
- Specifies the exemption in question.

The information provided to the applicant will be in the format that they have requested, where possible.

Where it is not possible to provide the information in the requested format, the School will assist the applicant by discussing alternative formats in which it can be provided.

The information provided will also be in the language in which it is held, or another language that is legally required. If the School is required to translate any information, it will do so.

If, under relevant disability and discrimination regulations, the School is legally obliged to provide the information in other forms and formats, it will do so.

4. The appropriate limit

The School will not comply with any freedom of information request that exceeds the statutorily imposed appropriate limit of £450 (18 hours).

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

- Determining whether it holds the information.
- Locating the information, or a document which may contain the information.
- Retrieving the information, or a document which may contain the information.
- Extracting the information from a document containing it.
- Costs related to the time spent by any person undertaking any of the activities outlined in section 4.2 of this policy on behalf of the School, are to be estimated at a rate of £25 per person per hour.

Where multiple requests for information are made to the School within 60 consecutive working days of each other, either by a single person or by different persons who appear to be acting in concert, the estimated cost of complying with any of the requests is to be taken to be the total costs to the School of complying with all of them.

5. Charging fees

The School may, within 20 working days, give an applicant who has requested information from the School, a written notice stating that a fee is to be charged for the School's compliance.

Charges may be made for disbursements, such as the following:

- Photocopying.
- Postage and packaging.

- Costs directly incurred as a result of viewing information.

Fees charged will not exceed the total cost to the School of:

- Informing the person making the request whether we hold the information.
- Communicating the information to the person making the request.

Where a fee is to be charged, the School will not comply with section 3 of this policy unless the requested fee is paid within a period of three months, beginning with the day on which the fees notice is given to the applicant.

The School will not take into account any costs which are attributable to the time spent by persons undertaking any of the activities mentioned in section 5.3 above.

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

6. Means by which communication is to be made

Where, on making a request for information, the applicant expresses a preference for communication by any one of the following means, the School will, as far as is practicable, give effect to that preference:

- The provision to the applicant of a copy of the information in permanent form or in another form acceptable to the applicant.
- The provision to the applicant of a reasonable opportunity to inspect a record containing the information.
- The provision to the applicant of a digest, or summary of the information, in permanent form or in another form acceptable to the applicant.

7. Providing advice and assistance

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

The School may offer advice and assistance in the following circumstances:

1. If an individual requests to know what types of information the School holds and the format in which it is available, as well as information on the fees regulations and charging procedures.
2. If a request has been made, but the School is unable to regard it as a valid request due to insufficient information, leading to an inability to identify and locate the information.
3. If a request has been refused, e.g. due to an excessive cost, and it is necessary for the School to assist the individual who has submitted the request.

The School will provide assistance for each individual on a case-by-case basis; examples of how the School will provide assistance include the following:

- Informing an applicant of their rights under the Freedom of Information Act 2000.
- Assisting an individual in the focus of their request, e.g. by advising of the types of information available within the requested category.
- Advising an applicant if information is available elsewhere and how to access this information.
- Keeping an applicant informed on the progress of their request.

In order to provide assistance as outlined above, the School will engage in the following good practice procedures:

- Make early contact with an individual and keep them informed of the process of their request.
- Accurately record and document all correspondence concerning the clarification and handling of any request.
- Give consideration to the most appropriate means of contacting the applicant, taking into account their individual circumstances.
- Discuss with the applicant whether they would prefer to receive the information in an alternative format, in cases where it is not possible to provide the information requested in the manner originally specified.
- Remain prepared to assist an applicant who has had their request denied due to an exemption.

The School will give particular consideration to what level of assistance is required for an applicant who has difficulty submitting a written request.

In circumstances where an applicant has difficulty submitting a written request, the School will:

- Make a note of the application over the telephone and then send the note to the applicant to confirm and return - the statutory time limit for a reply would begin here.
- Direct the individual to a different agency that may be able to assist with their request.

NB. This list is not exhaustive and the School may decide to take additional assistance measures that are appropriate to the case.

Where an applicant's request has been refused either because the information is accessible by other means, or the information is intended for future publication or research, the School, as a matter of good practice, will provide advice and assistance.

The School will advise the applicant how and where information can be obtained, if it is accessible by other means.

Where there is an intention to publish the information in the future, the School will advise the applicant of when this publication is expected.

If the request is not clear, the School will ask for more detail from the applicant in order to identify and locate the relevant information, before providing further advice and assistance.

If the School is able to clearly identify the elements of a request, it will respond following usual procedures and will provide advice and assistance for the remainder of the request.

If any additional clarification is needed for the remainder of a request, the School will ensure there is no delay in asking for further information.

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

If the School is under any doubt that the applicant did not receive the advice and assistance, the School will re-issue it.

The School is not required to provide assistance where an applicant's request is vexatious or repeated, as defined under section 14 of the Freedom of Information Act 2000.

The School is also not required to provide information where the cost of complying with a request exceeds the limit outlined in the Freedom of Information Act 2000. In such cases, the School will consider whether any information can be provided free of charge if the applicant refuses to pay the fee.

A record will be kept by the Headteacher in the school office of all the advice and assistance provided.

Publication scheme

The School will meet its duty to adopt and maintain a publication scheme which specifies the information which it will publish on the School website, and whether the information will be available free of charge or on payment.

The publication scheme will be reviewed and, where necessary, updated on an annual basis.

Monitoring and review

This policy will be reviewed on an annual basis, or in light of any changes to relevant legislation, by the Headteacher.

The next scheduled review date for this policy is **Spring 2024**

Model Publication Scheme

This scheme follows the model approved by the ICO and sets out the classes of information which we publish or intend to publish; the format in which the information will be made available and whether the information is available free of charge or on payment.

Classes of information

Information that is available under this scheme includes:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing?
- How we make decisions
- Our policies and procedures
- Lists and registers
- The services we offer

Information which **will not** be made available under this scheme includes:

- 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, or notes, documents in older versions, emails or other correspondence.
- 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.

Information to be published. This includes datasets where applicable - please see “How to complete the Guide to Information”.	How the information can be obtained
Class 1 - Who we are and what we do (Organisational information, structures, locations and contacts) This will be current information only	(hard copy and/or website)
Who's who in the school	Website
Who's who on the governing body and the basis of their appointment	Website
Instrument of Government	Hard copy
Contact details for the Headteacher and for the governing body, via the school (named contacts where possible).	Website
School prospectus (if any)	Website
Annual Report (if any)	Website
Staffing structure	Website / Hard copy
School session times and term dates	Website
Address of school and contact details, including email addresses.	Website
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	(hard copy and/or website)
Annual budget plan and financial statements	Hard copy
Capital funding	Hard copy
Financial audit reports	Hard copy
Details of expenditure items over £2000 – published at least annually but at a more frequent quarterly or six-monthly interval where practical.	Hard copy
Procurement and contracts the school has entered into, or information relating to / a link to information held by an organisation which has done so on its behalf (for example, a local authority or diocese).	Hard copy

Pay policy	Email
Staff allowances and expenses that can be incurred or claimed; with totals paid to individual senior staff members (Senior Leadership Team or equivalent, whose basic actual salary is at least £60,000 per annum) by reference to categories.	Hard copy
Staffing, pay and grading structure. As a minimum the pay information should include salaries for senior staff (Senior Leadership Team or equivalent as above) in bands of £10,000; for more junior posts, by salary range.	Hard copy
Governors' allowances that can be incurred or claimed, and a record of total payments made to individual governors.	Hard copy
Class 3 – What our priorities are and how we are doing (Strategies and plans, performance indicators, audits, inspections and reviews) Current information as a minimum	(hard copy or website)
School profile (if any) And in all cases: <ul style="list-style-type: none"> • Performance data supplied to the English Government or a direct link to the data 	Website
<ul style="list-style-type: none"> • The latest Ofsted / Estyn / Education and Training Inspectorate report <ul style="list-style-type: none"> - Summary - Full report 	Website
<ul style="list-style-type: none"> • Post-inspection action plan 	Email
Performance management policy and procedures adopted by the governing body.	Email
Performance data or a direct link to it	Website
The school's future plans; for example, proposals for and any consultation on the future of the school, such as a change in status	Website
Safeguarding and child protection	Website
Class 4 – How we make decisions (Decision making processes and records of decisions) Current and previous three years as a minimum	(hard copy or website)
Admissions policy/decisions (not individual admission decisions) – where applicable	Website

Agendas and minutes of meetings of the governing body and its committees. (NB this will exclude information that is properly regarded as private to the meetings).	Hard copy
<p>Class 5 – Our policies and procedures (Current written protocols, policies and procedures for delivering our services and responsibilities) Current information only. As a minimum these must include policies, procedures and documents that the school is required to have by statute or by its funding agreement or equivalent, or by the English government. These will include policies and procedures for handling information requests.</p>	(hard copy or website) Website
<p>Records management and personal data policies, including:</p> <ul style="list-style-type: none"> • Information security policies • Records retention, destruction and archive policies • Data protection (including information sharing policies) 	Website
<p>Charging regimes and policies.</p> <p>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. If the school charges a fee for re-licensing the use of datasets, it should state in its guide how this is calculated (please see “How to complete the Guide to information”).</p>	Website
<p>Class 6 – Lists and Registers Currently maintained lists and registers only (this does not include the attendance register).</p>	(hard copy or website; some information may only be available by inspection)
Curriculum circulars and statutory instruments	Hard copy
Disclosure logs	Hard copy
Asset register	Hard copy
Any information the school is currently legally required to hold in publicly available registers	Hard copy

Class 7 – The services we offer (Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses) Current information only	(hard copy or website; some information may only be available by inspection)
Services for which the school is entitled to recover a fee, together with those fees	Website
School publications, leaflets, books and newsletters	Hard copy

How to request information

Requested documents under this scheme will be delivered electronically where possible, but paper copies can be provided by contacting the school using the below contact details.

Email: DPO@greenparkschool.co.uk

Contact Address: Green Park School, Green Park Avenue, Bilston, WV14 6EH

To help us process your request quickly, please clearly mark any correspondence **“FREEDOM OF INFORMATION REQUEST”**

Documents can be translated under disability legislation into accessible formats where possible.

Charges

Documents contained in this scheme are free to view on the school website.

Single paper copies are also available free of charge to parents/carers and prospective parents/carers of the school.

<u>Type of charge</u>	<u>Description</u>	<u>Basis of charge</u>
Disbursement cost	Photocopying / printing per sheet (black & white) A4 / A3	Actual cost *
	Photocopying / printing per sheet (colour) A4 / A3	Actual cost *
	Postage (standard/large letter)	Actual cost of Royal Mail standard 2nd class * Actual cost of special / recorded delivery where requested / required *

* The actual cost incurred by the public authority.

Feedback

We welcome any comments or suggestions you may have regarding this scheme. Please contact the governing body using the following contact details:
greenparkschool@wolverhampton.gov.uk