





**Perseverance** **Respect** **Honesty** **Friendship**

# GDPR

|   |  |  |   |
|---|--|--|---|
| <b>Date written</b>   | <b>Authorised by</b>   | <b>Review Date</b>   |   |
| June 2022   | Governors  | June 2023  |   |
| <br>PERSEVERANCE | <br>RESPECT | <br>HONESTY | <br>FRIENDSHIP |



## Contents

|  |    |
|--|----|
| Introduction                           | 3  |
| GDPR/Data Protection                   | 4  |
| Data Breach                            | 15 |
| Data Retention                         | 21 |
| Freedom of Information and Publication | 57 |
| Information Security                   | 67 |
| Privacy                                | 72 |

## I Introduction

Brooklands Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Brooklands Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy is based on our four school values:



Our children are confident learners with strong core skills across the curriculum and they work hard to succeed with every challenge.



Our children show respect for themselves and other people in our community, our country and our world.



Our children understand the importance of being honest to themselves and others about their good choices and their mistakes.



Our children develop strong friendships with their peers and act in a friendly manner towards others. They understand the difference between these and are open to making new friendships.

## 2 GDPR/Data Protection



## Legal framework

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

- The General Data Protection Regulation (GDPR)

The Freedom of Information Act 2000

The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'

Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following other school policies:

- Photograph permissions
- E-safety Policy

## Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to



implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

### **Accountability**

Brooklands Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

### **Data protection officer (DPO)**

A DPO will be appointed in order to:

Inform and advise the school and its employees about their obligations to comply with GDPR and other data protection laws.

Monitor the school’s compliance with GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.



An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests. Our Data Protection Officer is the School Business Manager who can be contacted on 0161 973 3758 or [secretary@brooklands.trafford.sch.uk](mailto:secretary@brooklands.trafford.sch.uk)

The DPO will report to the highest level of management at the school, which is the headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

### Lawful processing

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

The school will act as a data processor; however, this role may also be undertaken by other third parties.

Under GDPR, data will be lawfully processed under the following conditions:

The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.



Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- 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 and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

## The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The contact details of the controller (the school), and where applicable, the controller's representative, as well as the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

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

## The right to rectification





Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

### **The right to erasure**

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.



Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

### **The right to restrict processing**

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

### **The right to data portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.



Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

### **The right to object**

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

### **Automated decision making and profiling**

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact. Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

### **Privacy by design and privacy impact assessments**

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.



A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

### **Data security**

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for school purposes.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.



Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

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

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Brooklands Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The school business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

### **Publication of information**

Classes of information specified in the publication scheme are made available quickly and easily on request.

Brooklands Primary School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

### **CCTV and photography**

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.



The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Precautions, as outlined in the photograph consent policy, are taken when publishing photographs of pupils, in print, video or on the school website.

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

### **DBS data**

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

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

## **3 Data Breach**

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

### **Personal Data Breach**

Person to whom the personal data relates.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

### **ICO**

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

### **Responsibility**

The Headteacher has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches. In the absence of the Headteacher, please contact the School Business Manager.



The Data Protection Officer (DPO) is responsible for overseeing and developing data-related policies and guidelines.

Please contact the DPO (School Business Manager) with any questions or if you have any concerns that this policy is not being or has not been followed.

## **Data Protection**

Data Protection sets out the School's obligations under GDPR about how they process personal data and is designed to protect personal data and can be found in the staff room or copies can be obtained from the school office.

## **Data Breach Procedure**

### **What Is A Personal Data Breach?**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

### **When Does It Need To Be Reported?**

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;





- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

## Reporting a Data Breach

Within a breach notification, the following information will be outlined:

The nature of the personal data breach, including the categories and approximate number of individuals and records concerned

The name and contact details of the DPO

An explanation of the likely consequences of the personal data breach

A description of the proposed measures to be taken to deal with the personal data breach

Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (which can be obtained from the Headteacher);
- Email the completed form to the Headteacher.

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the Headteacher or the School Business Manager.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Headteacher will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the School Business Manager.

## Managing and Recording The Breach



On being notified of a suspected personal data breach, the Headteacher will notify the School Business Manager. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

## Notifying the ICO

The Headteacher will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e. it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption will be to report it. Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

## Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Headteacher will notify the affected individuals without undue delay including the name and contact details of the School Business Manager and ICO, the likely consequences of the data breach and the measures the School have (or intend) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Headteacher will co-operate with and seek guidance from the School Business Manager, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

## Notifying Other Authorities



The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

## **Assessing The Breach**

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

## **Preventing Future Breaches**

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;



- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it's necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

## Reporting security breaches

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the School Business Manager. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of Trafford ICT Support.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Headteacher/School Business Manager.

All IT security breaches shall be fully documented.

## Reporting Data Protection Concerns

Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Headteacher or the School Business Manager. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

## Monitoring

We will monitor the effectiveness of these procedures and will conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

## 5 DATA RETENTION

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

School reflects its current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

### DATA PROTECTION

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Data will be stored and processed to allow for the efficient operation of the School.

### RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by the School Business Manager.



Electronic records will be regularly monitored by the School Business Manager.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

## **DESTRUCTION OF RECORDS**

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information will be shredded by an appropriate waste paper merchant. All electronic information will be deleted.

## **ARCHIVING**

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the School Business Manager. The appropriate staff member, when archiving documents should record in this list the following information: -

- File title/description;
- Number of files; and

## **TRANSFERRING INFORMATION TO OTHER MEDIA**

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.



## RESPONSIBILITY AND MONITORING

The School Business Manager has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

| Brooklands Primary School Retention Schedule |                        |                  |   |                                |  |  |
|--|------------------------|------------------|---|--------------------------------|--|--|
|  | Basic file description | Data Prot Issues | Statutory Provisions  | Retention Period [operational] | Action at the end of the administrative life of the record |  |
| 1.1  | Child Protection files | Yes              | Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004 | DOB + 25 years <sup>1</sup>    | SHRED  | Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example)<br><br>Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority. |

<sup>1</sup> This amendment has been made in consultation with the Safeguarding Children Group.

## Brooklands Primary School Retention Schedule

|     | Basic file description   | Data Prot Issues | Statutory Provisions  | Retention Period [operational]  | Action at the end of the administrative life of the record |  |
|-----|--|------------------|---|---|--|--|
| 1.2 | Allegation of a child protection nature against a member of staff, including where the allegation is unfounded | Yes              | <p>Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance)</p> <p>Education Act 2002 guidance “Dealing with Allegations of Abuse against Teachers and Other Staff” November 2005</p> | Until the person’s normal retirement age, or 10 years from the date of the allegation whichever is the longer | SHRED  | <p>The following is an extract from “Safeguarding Children and Safer Recruitment in Education” p60</p> <p>“Record Keeping</p> <p>5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person’s confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a</p> |



### Brooklands Primary School Retention Schedule

|  | Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record |   |
|--|------------------------|------------------|----------------------|--------------------------------|--|---|
|  |                        |                  |                      |                                |  | period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer.” |

### Governors

|     | Basic file description   | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record |                      |
|-----|--|------------------|----------------------|--------------------------------|--|----------------------|
| 2.1 | Minutes  |                  |                      |                                |  |                      |
|     | <ul style="list-style-type: none"> <li>Principal set (signed)</li> </ul> | No               |                      | Permanent                      | Retain in school for 6 years from date of meeting          | Transfer to Archives |

| <b>Governors</b> |  |                         |                             |                                       |  |  |
|------------------|--|-------------------------|-----------------------------|---------------------------------------|--|--|
|                  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b>                              |  |
|                  | <ul style="list-style-type: none"> <li><i>Inspection copies</i></li> </ul> | No                      |                             | Date of meeting + 3 years             | SHRED<br>[If these minutes contain any sensitive personal information they should be shredded] |  |
| 2.2              | Agendas  | No                      |                             | Date of meeting                       | SHRED  |  |
| 2.3              | Reports  | No                      |                             | Date of report + 6 years              | Retain in school for 6 years from date of meeting  | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 2.4              | Annual Parents' meeting papers   | No                      |                             | Date of meeting + 6 years             | Retain in school for 6 years from date of meeting  | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 2.5              | Instruments of Government  | No                      |                             | Permanent                             | Retain in school whilst school is open   | Transfer to Archives when the school has closed  |

| <b>Governors</b> |                               |                         |                             |   |  |   |
|------------------|-------------------------------|-------------------------|-----------------------------|---|--|---|
|                  | <b>Basic file description</b> | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>     | <b>Action at the end of the administrative life of the record</b>  |   |
| 2.6              | Trusts and Endowments         | No                      |                             | Permanent                                 | Retain in school whilst operationally required   | Transfer to Archives  |
| 2.7              | Action Plans                  | No                      |                             | Date of action plan + 3 years             | SHRED  | It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period |
| 2.8              | Policy documents              | No                      |                             | Expiry of policy                          | Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)                    | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation]                    |
| 2.9              | Complaints files              | Yes                     |                             | Date of resolution of complaint + 6 years | Retain in school for the first six years<br><br>Review for further retention in the case of contentious disputes<br><br>SHRED routine complaints |   |

| <b>Governors</b> |   |                         |                             |  |   |  |
|------------------|---|-------------------------|-----------------------------|--|---|--|
|                  | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>  | <b>Action at the end of the administrative life of the record</b> |  |
| 2.10             | Annual Reports required by the Department for Education and Skills              | No                      |                             | Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171 | Date of report + 10 years   | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 2.11             | Proposals for schools to become, or be established as Specialist Status schools | No                      |                             |  | Current year + 3 years  | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |

| <b>3 Management</b> |   |                         |                             |  |   |  |
|---------------------|---|-------------------------|-----------------------------|--|---|--|
|                     | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>    | <b>Action at the end of the administrative life of the record</b> |  |
| 3.1                 | Log Books   | Yes <sup>2</sup>        |                             | Date of last entry in the book + 6 years | Retain in the school for 6 years from the date of the last entry. | Transfer to the Archives   |
| 3.2                 | Minutes of the Senior Management Team and other internal administrative bodies  | Yes <sup>1</sup>        |                             | Date of meeting + 5 years                | Retain in the school for 5 years from meeting                     | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 3.3                 | Reports made by the head teacher or the management team   | Yes <sup>1</sup>        |                             | Date of report + 3 years                 | Retain in the school for 3 years from meeting                     | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 3.4                 | Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | Yes <sup>1</sup>        |                             | Closure of file + 6 years                | SHRED   |  |

<sup>2</sup> From January 1<sup>st</sup> 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.

| <b>3 Management</b> |  |                         |                             |                                       |   |                       |
|---------------------|--|-------------------------|-----------------------------|---------------------------------------|---|-----------------------|
|                     | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |                       |
| 3.5                 | Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | No                      |                             | Date of correspondence + 3 years      | SHRED   |                       |
| 3.6                 | Professional development plans   | Yes                     |                             | Closure + 6 years                     | SHRED   |                       |
| 3.7                 | School development plans   | No                      |                             | Closure + 6 years                     | Review  | Offer to the Archives |
| 3.8                 | Admissions – if the admission is successful  | Yes                     |                             | Admission + 1 year                    | SHRED   |                       |
| 3.9                 | Admissions – if the appeal is unsuccessful   | Yes                     |                             | Resolution of case + 1 year           | SHRED   |                       |
| 3.10                | Proofs of address supplied by parents as part of the admissions process  | Yes                     |                             | Current year + 1 year                 | SHRED   |                       |

| 4 Pupils |   |                  |                      |   |   |                          |
|----------|---|------------------|----------------------|---|---|--------------------------|
|          | Basic file description                                    | Data Prot Issues | Statutory Provisions | Retention Period [operational]                                    | Action at the end of the administrative life of the record  |                          |
| 4.1      | Admission Registers                                       | Yes              |                      | Date of last entry in the book (or file) + 6 years                | Retain in the school for 6 years from the date of the last entry.   | Transfer to the Archives |
| 4.2      | Attendance registers                                      | Yes              |                      | Date of register + 3 years  | SHRED<br>[If these records are retained electronically any back up copies should be destroyed at the same time]   |                          |
| 4.3      | Pupil record cards  | Yes              |                      |   |   |                          |
| 4.3      | <ul style="list-style-type: none"> <li>Primary</li> </ul> |                  |                      | Retain for the time which the pupil remains at the primary school | Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service |                          |

| 4 Pupils |   |                  |                      |   |  |  |
|----------|---|------------------|----------------------|---|--|--|
|          | Basic file description                                    | Data Prot Issues | Statutory Provisions | Retention Period [operational]                                    | Action at the end of the administrative life of the record   |  |
| 4.4      | Pupil files   | Yes              |                      |   |  |  |
| 4.4a     | <ul style="list-style-type: none"> <li>Primary</li> </ul> |                  |                      | Retain for the time which the pupil remains at the primary school | Transfer to the secondary school (or other primary school) when the child leaves the school.<br><br>In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service |  |



| 4 Pupils |   |                  |                      |  |  |  |
|----------|---|------------------|----------------------|--|--|--|
|          | Basic file description  | Data Prot Issues | Statutory Provisions | Retention Period [operational]   | Action at the end of the administrative life of the record |  |
| 4.5      | Special Educational Needs files, reviews and Individual Education Plans | Yes              |                      | DOB of the pupil + 25 years the review<br><br>NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period. | SHRED  |  |
| 4.6      | Letters authorising absence   | No               |                      | Date of absence + 2 years  | SHRED  |  |
| 4.7      | Absence books   |                  |                      | Current year + 6 years   | SHRED  |  |
| 4.8      | Examination results   | Yes              |                      |  |  |  |

| 4 Pupils |  |                  |                      |                                     |  |   |
|----------|--|------------------|----------------------|-------------------------------------|--|---|
|          | Basic file description   | Data Prot Issues | Statutory Provisions | Retention Period [operational]      | Action at the end of the administrative life of the record                           |   |
| 4.8a     | <ul style="list-style-type: none"> <li>Public</li> </ul>                       | No               |                      | Year of examinations + 6 years      | SHRED  | Any certificates left unclaimed should be returned to the appropriate Examination Board |
| 4.8b     | <ul style="list-style-type: none"> <li>Internal examination results</li> </ul> | Yes              |                      | Current year + 5 years <sup>3</sup> | SHRED  |   |
| 4.9      | Any other records created in the course of contact with pupils                 | Yes/No           |                      | Current year + 3 years              | Review at the end of 3 years and either allocate a further retention period or SHRED |   |

<sup>3</sup> If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

| <b>4 Pupils</b> |   |                         |  |                                       |   |  |
|-----------------|---|-------------------------|--|---------------------------------------|---|--|
|                 | <b>Basic file description</b>                                   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b>                                  | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |  |
| 4.10            | Statement maintained under The Education Act 1996 - Section 324 | Yes                     | Special Educational Needs and Disability Act 2001 Section 1  | DOB + 30 years                        | SHRED unless legal action is pending                              |  |
| 4.11            | Proposed statement or amended statement                         | Yes                     | Special Educational Needs and Disability Act 2001 Section 1  | DOB + 30 years                        | SHRED unless legal action is pending                              |  |
| 4.12            | Advice and information to parents regarding educational needs   | Yes                     | Special Educational Needs and Disability Act 2001 Section 2  | Closure + 12 years                    | SHRED unless legal action is pending                              |  |
| 4.13            | Accessibility Strategy  | Yes                     | Special Educational Needs and Disability Act 2001 Section 14 | Closure + 12 years                    | SHRED unless legal action is pending                              |  |

| <b>4 Pupils</b> |   |                         |                             |   |   |  |
|-----------------|---|-------------------------|-----------------------------|---|---|--|
|                 | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>   | <b>Action at the end of the administrative life of the record</b> |  |
| 4.14            | Children's SEN Files  | Yes                     |                             | DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases  | SHRED unless legal action is pending                              |  |
| 4.15            | Parental permission slips for school trips – where there has been no major incident | Yes                     |                             | Conclusion of the trip  | SHRED   |  |
| 4.16            | Parental permission slips for school trips – where there has been a major incident  | Yes                     | Limitation Act 1980         | DOB of the pupil involved in the incident + 25 years<br><br>The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils | SHRED   |  |

| 4 Pupils |   |                  |   |  |   |                          |
|----------|---|------------------|---|--|---|--------------------------|
|          | Basic file description  | Data Prot Issues | Statutory Provisions  | Retention Period [operational]   | Action at the end of the administrative life of the record  |                          |
| 4.17     | Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools | N                | 3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998). | Date of visit + 14 years <sup>4</sup>  | N   | SHRED or delete securely |
| 4.18     | Walking Bus registers   | Yes              |   | Date of register + 3 years<br><br>This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting | SHRED<br><br>[If these records are retained electronically any back up copies should be destroyed at the same time] |                          |

<sup>4</sup> This retention period has been set in agreement with the Safeguarding Children's Officer

| <b>5 Curriculum</b> |                               |                         |                             |                                       |  |
|---------------------|-------------------------------|-------------------------|-----------------------------|---------------------------------------|--|
|                     | <b>Basic file description</b> | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b>  |
| 5.1                 | Curriculum development        | No                      |                             | Current year + 6 years                | SHRED  |
| 5.2                 | Curriculum returns            | No                      |                             | Current year + 3 years                | SHRED  |
| 5.3                 | School syllabus               | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.4                 | Schemes of work               | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.5                 | Timetable                     | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.6                 | Class record books            | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.7                 | Mark Books                    | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |

| <b>5 Curriculum</b> |                               |                         |                             |                                       |  |
|---------------------|-------------------------------|-------------------------|-----------------------------|---------------------------------------|--|
|                     | <b>Basic file description</b> | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b>  |
| 5.8                 | Record of homework set        | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.9                 | Pupils' work                  | No                      |                             | Current year + 1 year                 | It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED |
| 5.10                | Examination results           | Yes                     |                             | Current year + 6 years                | SHRED  |
| 5.11                | SATS records                  | Yes                     |                             | Current year + 6 years                | SHRED  |
| 5.12                | PAN reports                   | Yes                     |                             | Current year + 6 years                | SHRED  |
| 5.13                | Value added records           | Yes                     |                             | Current year + 6 years                | SHRED  |

| <b>6 Personnel Records held in Schools</b> |  |                         |  |                                       |   |
|--|--|-------------------------|--|---------------------------------------|---|
|  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b>  | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |
| 6.1  | Timesheets, sick pay   | Yes                     | Financial Regulations  | Current year + 6 years                | SHRED   |
| 6.2  | Staff Personal files   | Yes                     |  | Termination + 7 years                 | SHRED   |
| 6.3  | Interview notes and recruitment records  | Yes                     |  | Date of interview + 6 months          | SHRED   |
| 6.4  | Pre-employment vetting information (including CRB checks)                            | No                      | CRB guidelines   | Date of check + 6 months              | SHRED<br>[by the designated member of staff]                      |
| 6.5  | Disciplinary proceedings:  | Yes                     | <b>Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.</b> |                                       |   |
| 6.5a                                       | <ul style="list-style-type: none"> <li><i>oral warning</i></li> </ul>                |                         |  | Date of warning + 6 months            | SHRED <sup>5</sup>  |
| 6.5b                                       | <ul style="list-style-type: none"> <li><i>written warning – level one</i></li> </ul> |                         |  | Date of warning + 6 months            | SHRED   |
| 6.5c                                       | <ul style="list-style-type: none"> <li><i>written warning – level two</i></li> </ul> |                         |  | Date of warning + 12 months           | SHRED   |

<sup>5</sup> If this is placed on a personal file it must be weeded from the file.



| <b>6 Personnel Records held in Schools</b> |   |                         |   |  |   |
|--|---|-------------------------|---|--|---|
|  | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b>   | <b>Retention Period [operational]</b>  | <b>Action at the end of the administrative life of the record</b> |
| 6.5d                                       | <ul style="list-style-type: none"> <li><i>final warning</i></li> </ul>  |                         |   | Date of warning + 18 months  | SHRED   |
| 6.5e                                       | <ul style="list-style-type: none"> <li><i>case not found</i></li> </ul> |                         |   | If child protection related please see 1.2 otherwise shred immediately at the conclusion of the case               | SHRED   |
| 6.6  | Records relating to accident/injury at work                             | Yes                     |   | Date of incident + 12 years<br>In the case of serious accidents a further retention period will need to be applied | SHRED   |
| 6.7  | Annual appraisal/assessment records                                     | No                      |   | Current year + 5 years   | SHRED   |
| 6.8  | Salary cards  | Yes                     |   | Last date of employment + 85 years   | SHRED   |
| 6.9  | Maternity pay records   | Yes                     | Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567) | Current year, +3yrs  | SHRED   |

| <b>6 Personnel Records held in Schools</b> |  |                         |                             |  |   |
|--|--|-------------------------|-----------------------------|--|---|
|  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>  | <b>Action at the end of the administrative life of the record</b> |
| 6.10                                       | Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995               | Yes                     |                             | Current year + 6 years   | SHRED   |
| 6.11                                       | Proofs of identity collected as part of the process of checking “portable” enhanced CRB disclosure | Yes                     |                             | Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file. |   |

| <b>7 Health and Safety</b> |   |                         |  |  |   |
|----------------------------|---|-------------------------|--|--|---|
|                            | <b>Basic file description</b>                                       | <b>Data Prot Issues</b> | <b>Statutory Provisions</b>  | <b>Retention Period [operational]</b>  | <b>Action at the end of the administrative life of the record</b> |
| 7.1                        | Accessibility Plans   |                         | Disability Discrimination Act  | Current year + 6 years   | SHRED   |
| 7.2                        | Accident Reporting  |                         | Social Security (Claims and Payments) Regulations 1979<br>Regulation 25. Social Security Administration Act 1992 Section 8.<br>Limitation Act 1980 |  |   |
| 7.2a                       | <ul style="list-style-type: none"> <li>• <i>Adults</i></li> </ul>   | Yes                     |  | Date of incident + 7 years   | SHRED   |
| 7.2b                       | <ul style="list-style-type: none"> <li>• <i>Children</i></li> </ul> | Yes                     |  | DOB of child + 25 years <sup>6</sup>   | SHRED   |
| 7.3                        | COSHH   |                         |  | Current year + 10 years<br>[where appropriate an additional retention period may be allocated] | SHRED   |
| 7.4                        | Incident reports  | Yes                     |  | Current year + 20 years  | SHRED   |
| 7.5                        | Policy Statements   |                         |  | Date of expiry + 1 year  | SHRED   |

<sup>6</sup> A child may make a claim for negligence for 7 years from their 18<sup>th</sup> birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.



## 7 Health and Safety

|     | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |
|-----|---|-------------------------|-----------------------------|---------------------------------------|---|
| 7.6 | Risk Assessments  |                         |                             | Current year + 3 years                | SHRED   |
| 7.7 | Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos |                         |                             | Last action + 40 years                | SHRED   |
| 7.8 | Process of monitoring of areas where employees and persons are likely to have come in contact with radiation  |                         |                             | Last action + 50 years                | SHRED   |
| 7.9 | Fire Precautions log books  |                         |                             | Current year + 6 years                | SHRED   |

## Administrative

|     | Basic file description                 | Data Prot Issues | Statutory Provisions | Retention Period [operational]   | Action at the end of the administrative life of the record   |  |
|-----|--|------------------|----------------------|----------------------------------|--|--|
| 8.1 | Employer's Liability certificate       |                  |                      | Closure of the school + 40 years | SHRED  |  |
| 8.2 | Inventories of equipment and furniture |                  |                      | Current year + 6 years           | SHRED  |  |
| 8.3 | General file series                    |                  |                      | Current year + 5 years           | Review to see whether a further retention period is required | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 8.4 | School brochure or prospectus          |                  |                      | Current year + 3 years           |  | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 8.5 | Circulars (staff/parents/pupils)       |                  |                      | Current year + 1 year            | SHRED  |  |

| <b>Administrative</b> |                               |                         |                             |                                       |   |  |
|-----------------------|-------------------------------|-------------------------|-----------------------------|---------------------------------------|---|--|
|                       | <b>Basic file description</b> | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |  |
| 8.6                   | Newsletters, ephemera         |                         |                             | Current year + 1 year                 | Review to see whether a further retention period is required      | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 8.7                   | Visitors book                 |                         |                             | Current year + 2 years                | Review to see whether a further retention period is required      | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 8.8                   | PTA/Old Pupils Associations   |                         |                             | Current year + 6 years                | Review to see whether a further retention period is required      | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |



**9 Finance**

|      | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>   | <b>Action at the end of the administrative life of the record</b> |  |
|------|--|-------------------------|-----------------------------|---|---|--|
| 9.1  | Annual Accounts  |                         | Financial Regulations       | Current year + 6 years                  |   | Offer to the Archives  |
| 9.2  | Loans and grants   |                         | Financial Regulations       | Date of last payment on loan + 12 years | Review to see whether a further retention period is required      | Transfer to Archives<br>[The appropriate archivist will then take a sample for permanent preservation] |
| 9.3  | Contracts  |                         |                             |   |   |  |
| 9.3a | <ul style="list-style-type: none"> <li>under seal</li> </ul>         |                         |                             | Contract completion date + 12 years     | SHRED   |  |
| 9.3b | <ul style="list-style-type: none"> <li>under signature</li> </ul>    |                         |                             | Contract completion date + 6 years      | SHRED   |  |
| 9.3c | <ul style="list-style-type: none"> <li>monitoring records</li> </ul> |                         |                             | Current year + 2 years                  | SHRED   |  |
| 9.4  | Copy orders  |                         |                             | Current year + 2 years                  | SHRED   |  |

| <b>9 Finance</b> |  |                         |                             |                                       |   |  |
|------------------|--|-------------------------|-----------------------------|---------------------------------------|---|--|
|                  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |  |
| 9.5              | Budget reports, budget monitoring etc                                    |                         |                             | Current year + 3 years                | SHRED   |  |
| 9.6              | Invoice, receipts and other records covered by the Financial Regulations |                         | Financial Regulations       | Current year + 6 years                | SHRED   |  |
| 9.7              | Annual Budget and background papers                                      |                         |                             | Current year + 6 years                | SHRED   |  |
| 9.8              | Order books and requisitions   |                         |                             | Current year + 6 years                | SHRED   |  |
| 9.9              | Delivery Documentation   |                         |                             | Current year + 6 years                | SHRED   |  |
| 9.10             | Debtors' Records   |                         | Limitation Act 1980         | Current year + 6 years                | SHRED   |  |
| 9.11             | School Fund – Cheque books   |                         |                             | Current year + 3 years                | SHRED   |  |
| 9.12             | School Fund – Paying in books  |                         |                             | Current year + 6 years then review    | SHRED   |  |



| <b>9 Finance</b> |  |                         |                             |                                       |   |  |
|------------------|--|-------------------------|-----------------------------|---------------------------------------|---|--|
|                  | <b>Basic file description</b>                            | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |  |
| 9.13             | School Fund – Ledger                                     |                         |                             | Current year + 6 years then review    | SHRED   |  |
| 9.14             | School Fund – Invoices                                   |                         |                             | Current year + 6 years then review    | SHRED   |  |
| 9.15             | School Fund – Receipts                                   |                         |                             | Current year + 6 years                | SHRED   |  |
| 9.16             | School Fund – Bank statements                            |                         |                             | Current year + 6 years then review    | SHRED   |  |
| 9.17             | School Fund – School Journey books                       |                         |                             | Current year + 6 years then review    | SHRED   |  |
| 9.18             | Applications for free school meals, travel, uniforms etc |                         |                             | Whilst child at school                | SHRED   |  |
| 9.19             | Student grant applications                               |                         |                             | Current year + 3 years                | SHRED   |  |
| 9.20             | Free school meals registers                              | Yes                     | Financial Regulations       | Current year + 6 years                | SHRED   |  |

| 9 Finance |                        |                  |                       |                                |  |  |
|-----------|------------------------|------------------|-----------------------|--------------------------------|--|--|
|           | Basic file description | Data Prot Issues | Statutory Provisions  | Retention Period [operational] | Action at the end of the administrative life of the record |  |
| 9.21      | Petty cash books       |                  | Financial Regulations | Current year + 6 years         | SHRED  |  |

| 10 Property |                        |                  |                      |                                |  |   |
|-------------|------------------------|------------------|----------------------|--------------------------------|--|---|
|             | Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational] | Action at the end of the administrative life of the record   |   |
| 10.1        | Title Deeds            |                  |                      | Permanent                      | Permanent<br>these should follow the property unless the property has been registered at the Land Registry | Offer to Archives if the deeds are no longer needed |
| 10.2        | Plans                  |                  |                      | Permanent                      | Retain in school whilst operational  | Offer to Archives <sup>7</sup>                      |

<sup>7</sup> If the property has been sold for private housing then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime.

| <b>10 Property</b> |  |                         |                             |                                       |   |  |
|--------------------|--|-------------------------|-----------------------------|---------------------------------------|---|--|
|                    | <b>Basic file description</b>              | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |  |
| 10.3               | Maintenance and contractors                |                         | Financial Regulations       | Current year + 6 years                | SHRED   |  |
| 10.4               | Leases                                     |                         |                             | Expiry of lease + 6 years             | SHRED   |  |
| 10.5               | Lettings                                   |                         |                             | Current year + 3 years                | SHRED   |  |
| 10.6               | Burglary, theft and vandalism report forms |                         |                             | Current year + 6 years                | SHRED   |  |
| 10.7               | Maintenance log books                      |                         |                             | Last entry + 10 years                 | SHRED   |  |
| 10.8               | Contractors' Reports                       |                         |                             | Current year + 6 years                | SHRED   |  |



## 11 Schools Meals

|      | <b>Basic file description</b> | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b> | <b>Action at the end of the administrative life of the record</b> |
|------|-------------------------------|-------------------------|-----------------------------|---------------------------------------|---|
| 11.1 | Dinner Register               |                         |                             | C + 3 years                           | SHRED   |
| 11.2 | School Meals Summary Sheets   |                         |                             | C + 3 years                           | SHRED   |

| <b>12 Early Years Provision</b>                                  |   |                         |                             |   |
|--|---|-------------------------|-----------------------------|---|
| <b>12.1 Records to be kept by Registered Persons - All Cases</b> |   |                         |                             |   |
|  | <b>Basic file description</b>   | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>   |
| 12.1.1   | The name, home address and date of birth of each child who is looked after on the premises                | Y                       |                             | Closure of setting + 50 years<br>[These could be required to show whether or not an individual child attended the setting in a child protection investigation]  |
| 12.1.2   | The name, home address and telephone number of a parent of each child who is looked after on the premises | Y                       |                             | If this information is kept in the same book or on the same form as in 16.1.1 then the same retention period should be used as in 16.1.1<br><br>If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact) |
| 12.1.3   | The name, address and telephone number of any person who will be looking after children on the premises   | Y                       |                             | See 16.4.5 below  |

| <b>12 Early Years Provision</b>                                  |  |                         |  |   |  |
|--|--|-------------------------|--|---|--|
| <b>12.1 Records to be kept by Registered Persons - All Cases</b> |  |                         |  |   |  |
|  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b>  | <b>Retention Period [operational]</b>   |  |
| 12.1.4   | A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them | Y                       | The Day Care and Child Minding (National Standards) (England) Regulations 2003 | The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). If these records are likely to be needed in a child protection setting (see 16.1.1 above) then the records should be retained for closure of setting + 50 years |  |
| 12.1.5   | A record of accidents occurring on the premises and incident books relating to other incidents   |                         | Y  | The Day Care and Child Minding (National Standards) (England) Regulations 2003 <sup>8</sup>   | DOB of the child involved in the accident or the incident + 25 years<br><br>If an adult is injured then the accident book must be kept for 7 years from the date of the incident |

<sup>8</sup> The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The Statute of Limitations states that a minor may make a claim for 7 years from their eighteenth birthday, therefore the retention should be for the longer period.

| <b>12 Early Years Provision</b>                                  |  |                         |                             |   |   |
|--|--|-------------------------|-----------------------------|---|---|
| <b>12.1 Records to be kept by Registered Persons - All Cases</b> |  |                         |                             |   |   |
|  | <b>Basic file description</b>  | <b>Data Prot Issues</b> | <b>Statutory Provisions</b> | <b>Retention Period [operational]</b>   |   |
| 12.1.6   | A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent | Y                       |                             | The Day Care and Child Minding (National Standards) (England) Regulations 2003 <sup>9</sup> | DOB of the child being given/taking the medicine + 25 years   |
| 12.1.7   | Records of transfer  | Y                       |                             |   | One copy is to be given to the parents, one copy transferred to the Primary School where the child is going |
| 12.1.8   | Portfolio of work, observations and so on  | Y                       |                             |   | To be sent home with the child  |

<sup>9</sup> The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The NHS records retention schedule states that any records relating to a child under the age of 18 should be retained until that child reaches the age of 25 years. Therefore, the retention should be DOB of the child being given/taking the medicine + 25 years



## 12 Early Years Provision

### 12.1 Records to be kept by Registered Persons - All Cases

|        | Basic file description | Data Prot Issues | Statutory Provisions | Retention Period [operational]   |
|--------|------------------------|------------------|----------------------|--|
| 12.1.9 | Birth certificates     |                  | Y                    | Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate. |



## **6 FREEDOM OF INFORMATION AND PUBLICATION SCHEME**

### **Introduction**

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information, and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public Authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

### **FREEDOM OF INFORMATION REQUESTS**

Requests under Freedom of Information should be made to the School Business Manager. However the request can be addressed to anyone in the School; so all staff need to be aware of the process for dealing with requests.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act: -

#### **Data Protection enquiries (or Subject Access Requests/SARs)**

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

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

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.



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

Environmental Information Regulations enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health, and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone masts, school playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests must be made in writing, (including email), and should include the enquirer's name, correspondence address (email addresses are allowed), and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the School require further information in order to deal with your request, the School will request this further information directly from the individual making the request. Please note that the School do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the School receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held, and supplying any information that is held, except where exemptions apply. There is a time limit of 20 school days (i.e. excluding school holidays) for responding to the request.

## Information

Provided all requirements are met for a valid request to be made, the School will provide the information that it holds (unless an exemption applies).

Holding information means information relating to the business of the school:

- That the school has created; or
- That the school has received from another body or person; or
- Held by another body on the school's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority, such as the Local Authority, first check with them they hold it, then transfer the request to them. If this applies, the School will notify the enquirer that they do not hold the information and to whom they have transferred the request. The School will continue to answer any parts of the enquiry in respect of information it does hold.

When the School does not hold the information, it has no duty to create or acquire it just to answer the enquiry; although a reasonable search will be made before confirming whether the School has the information requested.



If the information requested is already in the public domain, for instance, through the Publication Scheme or on the School's website, the School will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the School (subject to any of the exemptions). This obligation is known as the school's duty to confirm or deny that it holds the information. However, the school does not have to confirm or deny if:-

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

## Vexatious Requests

There is no obligation on the School to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the school. However, this does not provide an excuse for bad records management.

In addition, the School do not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

## Fees

The School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the school can only charge for the cost of informing the applicant whether the information is held, and communicating the information to the applicant (e.g. photocopying, printing and postage costs).

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information, and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit, (£450) the school can turn the request down, answer and charge a fee or answer and waive the fee.

If the School are going to charge they will send the enquirer a fees notice. The School do not have to comply with the request until the fee has been paid. More details on fees can be found on the ICO website.

If planning to turn down a request for cost reasons, or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

## Time Limits



Compliance with a request must be prompt and within the time limit of 20 school days (this does not include the school holidays or weekends) or 60 working days if this is shorter. Failure to comply could result in a complaint by the requester to the Information Commissioner's Office. The response time starts counting as the first day from the next working day after the request is received (so if a request was received on Monday 6<sup>th</sup> October the time limit would start from the next working day, the 7<sup>th</sup> October).

Where the School has asked the enquirer for more information to enable it to answer, the 20 school days start time begins when this further information has been received.

If some information is exempt this will be detailed in the School's response.

If a qualified exemption applies and the School need more time to consider the public interest test, the School will reply in 20 school days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the School has notified the enquirer that a charge is to be made, the time period stops until payment is received.

### **Third Party Data**

Consultation of third parties may be required if their interests could be affected by release of the information requested, and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the School to determine if information is exempt from disclosure; or
- The views of the third party may assist the School to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g. Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

### **Exemptions**

The presumption of the Freedom of Information Act is that the School will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The School may refuse all/part of a request, if one of the following applies: -

- 1) There is an exemption to disclosure within the act;
- 2) The information sought is not held;
- 3) The request is considered vexatious or repeated; or
- 4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are very specialised in their application (such as national security) and would not usually be relevant to schools.

There are two general categories of exemptions:-



- 1) Absolute: where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
- 2) Qualified: where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

### **Absolute Exemptions**

There are eight absolute exemptions set out in the Act. However the following are the only absolute exemptions which will apply to the School: -

- Information accessible to the enquirer by other means (for example by way of the School's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e. information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

### **Qualified Exemptions**

If one of the below exemptions apply (i.e. a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the School are: -

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);
- Reasons of National Security;
- Government/International Relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the School;
- Law enforcement (i.e. if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);
- Release of the information would prejudice the ability of the School to carry out an effective audit of its accounts, resources and functions;
- For Health and Safety purposes;
- Information requested is Environmental information;
- Information requested is subject to Legal professional privilege; and
- For Commercial Interest reasons.

Where the potential exemption is a qualified exemption, the School will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it.

In all cases, before writing to the enquirer, the person given responsibility by the School for dealing with the request will need to ensure that the case has been properly considered, and that the reasons for refusal, or public interest test refusal, are sound.

### **Refusal**

If it is decided to refuse a request, the School will send a refusals notice, which must contain



- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The School's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

### **Classes of Information**

There are six classes of information that we hold: -

- 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
- The services we offer

### **Making Information Available**

Information will generally be made available on the school website. Where it is not possible to include this information on the school website, or when an individual does not wish to access the information by the website the school will indicate how information can be obtained by other means and provide it by those means. This may be detailed in response to a request or within the scheme itself. This will usually be by way of a paper copy.

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

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

### **Charges for Information Published Under this Scheme**

The school may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum. Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law. Charges will be made to cover:

- Photocopying;
- Postage and Packaging; &
- The costs directly incurred as a result of viewing information.



Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case we will let you know as well as let you know the cost before fulfilling your request.

### How to request information

If you require a paper version of any of the documents within the scheme please contact the school using the contact details below.

Telephone: 0161 973 3758

Email: [secretary@brooklands.trafford.sch.uk](mailto:secretary@brooklands.trafford.sch.uk)

Address: Brooklands Primary School, Woodbourne Road, Sale, M33 3XS

Please mark all correspondence Publication Scheme Request in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the school to ask if we have this information.

### The Publication Schedule

| Who we are and what we do                  | Description   |
|--|---|
| Information relating to the Governing Body | Information contained in official governing body documents including the governor's annual report:- <ul style="list-style-type: none"><li>• Who is who</li><li>• Basis of governors appointment</li><li>• The manner in which the governing body is constituted</li><li>• Category of the school</li><li>• A statement on progress in implementing the action plan drawn up following an inspection</li><li>• Instruments of government, including the date it takes effect</li><li>• The term of office of each category of governor if it lasts less than 4 years and the name of anybody entitled to appoint any category of governor.</li></ul> |
| School website                             | <ul style="list-style-type: none"><li>• The name, address, website and telephone number of the school and the type of school</li><li>• The name of the school Headteacher</li></ul>   |

|  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• Information about the schools policy on providing for pupils with special educational needs</li> <li>• Statement on the schools aims and values</li> <li>• Information on the school policy on admissions</li> <li>• School term dates, times and attendance</li> <li>• Uniform</li> </ul> |
|--|---|

| What we spend and how we spend it | Description   |
|-----------------------------------|---|
| Pay policy                        | A copy of the pay policy that the school uses to govern staff pay.    |
| Allowances                        | Details of allowances and expenses that can be incurred by governors. |
| Pupil Premium                     | How the school uses pupil premium.                                    |
| PE & Sports Premium               | How the school uses PE & Sports Premium                               |

| What our priorities are and how we are doing | Description  |
|--|--|
| Ofsted report                                | A published report of the outcome of our latest Ofsted inspection  |
| Performance management Policy                | Statement of procedures adopted by the governing body relating to the performance management of staff and the annual report of the Headteacher on the effectiveness of appraisal procedures. |



|  |  |
|--|--|
| 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 publication, music tuition, trips. |
| 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.   |
| 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.   |

| How we make decisions                            | Description  |
|--|--|
| Admissions Policy/<br>Decisions (not individual) | This does not include individual decisions. This is a statement of our policy with regards to admissions and how we make decisions regarding admissions. |

| Our policies and procedures | Description  |
|-----------------------------|--|
| Home-School Agreement       | Written statements of the schools aims and values, the schools responsibilities, the parental responsibilities the schools expectations of its pupils. |
| Curriculum Policy           | Statement on following the national curriculum subjects, including any syllabus used by the school.  |

|  |   |
|--|---|
| Complaints Policy                        | Statement of procedures for dealing with complaints   |
| Equality and Diversity Policy            | Statement on ensuring that the school follows and promotes equality and diversity   |
| Child protection and safeguarding policy | Statement of policy for safeguarding and promoting welfare of pupils at the school.                                       |
| Relationships and Sex Education Policy   | Statement of policy with regard to sex and relationship education   |
| Inclusion Policy                         | Information about the school's policy on providing for pupils with special educational needs.                             |
| Behaviour Policy                         | Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying. |

| The services we offer                               | Description  |
|---|--|
| Extra-curricular Activities and out of school clubs | Details of these are contained on the school website |

### Complaints and/or Appeals

Any written (including email) expression of dissatisfaction should be handled through the School's existing complaints procedure. Wherever practicable the review should be handled by someone not involved in the original decision.

The Governing Body should set and publish a target time for determining complaints and information on the success rate in meeting the target. The school should maintain records of all complaints and their outcome.

If the outcome is that the School's original decision or action is upheld, then the applicant can appeal to the Information Commissioner. The appeal can be made via their website or in writing to:



Customer Contact  
Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
SK9 5AF

## 7 INFORMATION SECURITY

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This documents sets out the measures taken by the school to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they themselves handle.

### Introduction

Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

### Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

It applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.



Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## **General principles**

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the School Business Manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Trafford ICT Support or by such third party/parties as the School Business Manager may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the School Business Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the School Business Manager who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the School Business Manager.

## **Physical security and procedures**

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked cabinets in classrooms shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the School Business Manager as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

School carry's out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The gates are locked during school hours to prevent unauthorised access to the building. An alarm system is set nightly.

All visitors are required to sign in at reception, and never be left alone in areas where they could have access to confidential information.



## Computers and IT

### Responsibilities of Trafford ICT Support

Trafford ICT Support shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
- b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;
- c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, Trafford ICT Support shall be responsible for the following:

- a) assisting all members of staff in understanding and complying with this policy;
- b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
- d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the School Business Manager;
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

### Responsibilities – Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the School Business Manager of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

You are not entitled to install any software of your own without the approval of Trafford ICT Support. Any software belonging to you must be approved by Trafford ICT Support and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.



Prior to installation of any software onto the IT Systems, you must obtain permission from the Headteacher. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage USB memory sticks for transferring files, you must make sure the memory stick is encrypted.

If you detect any virus this must be reported immediately to Trafford ICT Support (this rule shall apply even where the anti-virus software automatically fixes the problem).

## Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by Trafford ICT Support.

All passwords must, where the software, computer, or device allows:

- a) be at least 6 characters long including both numbers and letters;
- b) be changed on a regular basis, at least every 180 days;
- c) cannot be the same as the previous 20 passwords you have used;
- d) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify Trafford ICT Support to have your access to the IT Systems reset. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

All mobile devices provided by the school, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password to unlock. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the



School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

## **Data security**

Personal data sent over the school network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Headteacher who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems.

All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies. The Headteacher may at any time request the immediate disconnection of any such devices without notice.

## **Electronic storage of data**

All portable data, and in particular personal data, should be stored on encrypted USB memory sticks recommended by the School Business Manager.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Headteacher. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by Trafford ICT Support.

## **Home working**

You should not take confidential or other information home without prior permission of the Headteacher, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- b) all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

## **Communications, transfer, internet and email use**



When using the School's IT Systems you are subject to and must comply with the Acceptable User Policy.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the School Business Manager.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email.

Postal and email addresses should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission from the Headteacher except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

## **8 Privacy**

### **Who processes your information?**

Brooklands Primary School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. The Headteacher acts as a representative for the school with regard to its data controller responsibilities; they can be contacted on 0161 973 3758 or [secretary@brooklands.trafford.sch.uk](mailto:secretary@brooklands.trafford.sch.uk)

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third party processor, the same data protection standards that Brooklands Primary School upholds are imposed on the processor

### **Why do we collect and use your information?**





Brooklands Primary School holds the legal 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, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013

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

### **Which data is collected?**

The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information
- Information relating to SEND
- Behavioural information – e.g. number of temporary exclusions

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, 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.

### **How long is your data stored for?**

Personal data relating to pupils at Brooklands Primary School and their families is stored in line with the school's GDPR 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.

### **Will my information be shared?**

The school is required to share pupils' data with the DfE on a statutory basis, this includes the following:

The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Brooklands Primary 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 NDP 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 NDP is maintained.

Brooklands Primary School will not share your personal information with any third parties without your consent, unless the law allows us to do so. The school routinely shares pupils' information with:

- Pupils' destinations upon leaving the school.
- Local Authority (LA).
- Groupcall- to provide effective communication via text/ email with Parents.
- ParentPay & The Evolve Hub- to provide a cashless system for Payment of school meals and trips.
- Evolve- system to provide the LA with details of school visits.
- Target Tracker- pupil's progress tracking service.
- Fronter – secure site for end of year results to be uploaded to DfE.
- Photographer – individual and class photographs taken.
- Earwig – assessment tool for early years through to Y4 children.
- Bug Club – Reading scheme.
- School Cloud- Parents evening bookings
- Spag.com – provides practise punctuation and grammar tests for KS1 & 2 children
- Travel tracker – tracking pupil's journeys.
- Social services – as required.
- NHS – flu vaccination consents.
- CPOMS- Safeguarding system used within school.
- Google Classroom



## **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:

- Be informed about how Brooklands Primary School uses your personal data.
- Request access to the personal data that Brooklands Primary School holds.
- 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.
- Request that the processing of your data is restricted.
- Object to your personal data being processed.

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

If you have a concern about the way Brooklands Primary School and/or the DfE is collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## **Where can you find out more information?**

If you would like to find out more information about how we and/or the DfE collect, use and store your personal data you can contact the school on 0161 973 3758 or [secretary@brooklands.trafford.sch.uk](mailto:secretary@brooklands.trafford.sch.uk)