



## GDPR DATA PROTECTION POLICY

The Willow Learning Trust collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust in order to provide education and associated functions. The WLT may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulations and other related legislation.

### 1. Legal framework

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

- The General Data Protection Regulation (2018) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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 also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'
- Protection of Freedoms Act 2012 when referring to our use of biometric data
- ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

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

- Photo and Video Policy
- Data Security Policy
- Freedom of Information Policy
- Data Retention Policy
- CCTV Policy

### 2. Applicable data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

**Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Sensitive data is given special protection and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The WLT does not intend to seek or hold sensitive personal data about staff or students except where the WLT has been notified of the information or it comes to WLT's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the WLT their race or ethnic origin, political or religious beliefs, whether or not they are trade union members or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes e.g. pension entitlements).

### **3. The Data Controller**

Our schools process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore The Trust is the data controller.

The Trust has paid its data protection fee to the ICO, as legally required.

### **4. Roles and Responsibilities**

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

The Board of Trustees has overall responsibility for ensuring that our Trust and schools comply with all relevant data protection obligations.

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

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

Our DPO is Mr S Hume and is contactable via email at [DPOfficer@glenthorne.sutton.sch.uk](mailto:DPOfficer@glenthorne.sutton.sch.uk)

Staff are responsible for:

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

### **5. 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.

In addition to this, the WLT is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". This will mean that the WLT will:

- Inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- Be responsible for checking the quality and accuracy of the information;
- Regularly review the records held to ensure that information is not held any longer than is necessary, and that it has been held in accordance with the data retention policy;
- Ensure that when information is authorised for disposal it is done appropriately;
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all time;
- Share personal information with others only when it is necessary and legally appropriate to do so;
- Set out clear procedures for responding to requests for access to personal information known as subject access requests;
- Report any breaches of the GDPR in accordance with the procedure detailed in this policy.

## **6. Lawful processing**

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

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

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given
- 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.

## 7. Use of personal data

The WLT holds personal data on pupils, staff and other individuals such as visitors and volunteers. In each case, their personal data must be treated in accordance with the data protection principles as outlined in paragraph 3 above.

The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, disciplinary reports and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the WLT as a whole is doing together with any other uses normally associated with this provision in a school environment.

In particular the WLT may:

- Transfer information to any association or society or club set up for the purpose of maintaining contact with pupils or for the fundraising, marketing or promotional purposes related to the WLT, but only where consent has been obtained first.
- Make personal data, including sensitive personal data, available to staff for planning curricular and extra-curricular activities;
- Keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the WLT to their previous school;
- Use photographs of pupils in accordance with the Photos and Videos policy.

The personal data held about staff will include contact details, employment history, information relating to career progression, information related to DBS checks and photographs. The data is used to comply with legal obligations placed under the WLT in relation to employment and the education of children in a school environment. The WLT may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material, but only where consent has been provided. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Protection Officer who will ensure that this is recorded, and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the WLT cannot comply with their request.

The WLT may hold personal information in relation to other individuals who have contact with the schools, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

**Biometric information** is information about a person's physical or behavioural characteristics that can be used to identify them, for example, their fingerprint. The WLT may use finger recognition to allow students or staff to identify themselves when paying for food in school. This is a totally secure system which significantly reduces queueing time and means we do not have to use plastic cards which are quickly damaged or lost. This system will take measurements of fingerprints and convert these measurements into a template to be stored on the system. Images of fingerprints are not stored. The template (i.e. measurements taken from fingerprints) is what will be used to permit access to services.

If biometric information is used within the WLT:

- we will comply with the requirements of the Protection of Freedoms Act 2012.
- Consent will be sought prior to its use in order to share the information with Cunningham's (the WLT's supplier of biometric systems);
- Parents/carers and pupils have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those pupils;
- The WLT will not use the information for any purpose other than those for which it was originally obtained and made known (i.e. as stated above);
- the WLT will ensure that the information is stored securely;
- A Data Processing Impact Assessment will be conducted to ensure the risk to personal data is minimised.

## **8. Consent**

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

Where consent is given, a record will be kept documenting how and when consent was given. The WLT ensures that consent mechanisms meet the standards of the 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.

Where a child is under 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.

## **9. Security of personal data**

The WLT will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. The WLT will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. For further details regarding the security of personal data please refer to the Data Security Policy.

## **10. Disclosure of data to third parties**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. The following list (whilst not exclusive) includes the most usual reasons that the WLT will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or pupil;
- For the prevention or detection of a crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the WLT (other than an obligation imposed by contract);
- For the purpose or, or in connection with legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damages or distress);
- To publish the results of public examinations other achievements of pupils of the WLT;
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of a school trip;
- To provide information to another educational establishment to which a pupil is transferring;
- To provide information to the Examination Authority as part of the examination process; and

- To provide information to the relevant Government Department concerned with national education. At the time of writing this Policy, this is the Department for Education (DfE).

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The WLT may receive requests from third parties (i.e. those other than the data subject, the WLT, and the WLT employees) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under UK data protection legislation which allow disclosures applies; or where necessary for the legitimate interests of the individual concerned or the WLT.

All requests for the disclosure of personal data must be sent to the Data Protection Officer, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

### **11. The right to be informed**

The privacy notice supplied to individuals informing them of 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 WLT 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 identity and contact details of the controller (and where applicable, the controller's representative) and 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 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.

### **12. The right of access**

Individuals have the right to obtain confirmation that their data is being processed. They 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. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure provided that they constitute a "filing system".

All SARs must be made in writing and should be sent to the DPO within 3 working days of receipt, and must be dealt with without delay and at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make his or her own request (usually under 13, or 13 or over but who lack sufficient understanding due to special educational needs), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that:

- The child or young person lacks sufficient understanding; and
- The request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their information rights, may appoint another person to request access to their records. In such circumstances the WLT must have written evidence of this authorisation. The WLT will verify the identity of the person making the request before any information is supplied.

Access to records will be refused in instances where an exemption applies, for example, where information sharing may place the individual at risk of significant harm or jeopardise police investigations in any alleged offence(s).

An individual only has the automatic right to access information about themselves. Care will be taken not to disclose the personal data of third parties where consent has not been given, or where it would not be appropriate to release the information.

A copy of the information will be supplied to the individual free of charge; however, the WLT may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

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 WLT 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 WLT will ask the individual to specify the information the request is in relation to. Further information about making a subject access request can be found in **Appendix 2**.

### **13. Parental requests to see the educational record**

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

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

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

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

### **14. The right to rectification**

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where any request for rectification is received, it should be sent to the DPO within two working days of receipt and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practical and the individual notified.

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

Where there is a dispute to the accuracy of the data, the request and reasons for refusals shall be noted alongside the data, and communicated to the individual. The individual can appeal to the Information Commissioner Office.

Where no action is being taken in response to a request for rectification, the WLT 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.

### **15. 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 DPO will make a decisions regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

### **16. The right to restrict processing**

Individuals have the right to block or suppress the WLT's processing of personal data. In the event that processing is restricted, the WLT 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 WLT 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 WLT has verified the accuracy of the data.
- Where an individual has objected to the processing and the WLT 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 WLT no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

### **17. The right to data portability**

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. If an individual wishes to send their personal data to another organisation they have the right to request that the WLT provides their information in a structured, commonly used and machine readable format. The WLT is not required to adopt or maintain processing systems which are technically compatible with other organisations.

The right to data portability only applies where the WLT is processing the information:

- on the basis of the individual's consent
- on the basis of the performance of a contract

The WLT will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. In the event that the personal data concerns

more than one individual, the WLT will consider whether providing the information would prejudice the rights of any other individual. The WLT 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 WLT 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.

### **18. The right to object**

The WLT will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice.

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 WLT will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the WLT 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 WLT will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The WLT 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 WLT is not required to comply with an objection to the processing of the data.

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

The WLT will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the WLT 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 WLT's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the WLT to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the WLT'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.

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

- 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 WLT 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 WLT will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

## **20. Data breaches**

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Headteachers will make all reasonable endeavours to ensure that there are no personal data breaches and will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

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

## **21. Publication of information**

The WLT publishes a publication scheme outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

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

The WLT will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

## **22. CCTV and photography**

The WLT understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We use CCTV in various locations around our school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

All CCTV footage will be kept for one month for security purposes; the WLT Headteachers are responsible for keeping the records secure and allowing access. Please refer to our CCTV Policy for the full code of practice.

Precautions, as outlined in the Photo and Videos Policy, are taken when publishing photographs of pupils, in print, video or on the schools' websites. We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Images and videos of individuals will not be published by the WLT without consent.

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

### **23. Data retention**

Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable in accordance with the Data Retention Policy.

### **24. 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.

### **25. Training**

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

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

### **26. Policy review**

This policy is reviewed every year by the DPO and the CEO and approved by the Trust Finance, Audit and Premises Committee.

The next scheduled review date for this policy is **May 2027**.

## **Appendix 1: Personal Data Breach Procedure**

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

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered to the DPO. Once notified the DPO shall assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information; and
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the DPO concludes that there is unlikely to be any risks to the individuals from the breach, it must be notified to the Information Commissions Office within 72 hours of the breach having come to the attention of the WLT, unless the delay can be justified.

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
- The decision to report to the ICO.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Staff will cooperate with the breach investigation (including allowing access to information and responding to questions). Failure to report a breach when required to do so may result in disciplinary action.

Records of all breaches will be stored on the a secure network and reported on as a standard agenda item at the Trust Finance and Premises committee. The DPO and Data Protection link Trustee will review the breaches to identify any trends or patterns requiring action by the school/Trust to reduce the risks of future breaches.

## **Appendix 2: Guide to making a Subject Access Request**

These notes are intended only as a guide to completing the Subject Access Request form, not as a guide to the Data Protection Act. The Data Protection law is set out in the Data Protection Act 2018. Further information and advice are also available from the website of the Data Protection Regulator – the Information Commissioner – see [www.ico.uk](http://www.ico.uk)

### **Your Rights**

Under the Act you have (subject to certain exemptions) the right to be told whether The Willow Learning Trust, as a Data Controller, is holding or processing any information about you; and if so, to be provided with a copy of that information upon specific request. The records covered by the Act include all computer records and limited categories of manual records. Under the Act a pupil, or someone acting on their behalf, has the right to access their personal information held by The Willow Learning Trust. The Trust's Data Protection Policy provides clarity on the age at which a pupil becomes the controller of their own data.

### **The Academy's Rights**

Where an exemption is available under the Act, the Trust may not provide you with the information covered by the exemption.

The main exemptions that may be applied are where the information held relates to:

- the prevention or detection of crime; or
- the apprehension or prosecution of offenders.

Where the disclosure of the information would be likely to prejudice any of these purposes the Trust is not required to tell you whether any exemptions have been applied to any information that the school may provide, or whether any information has been withheld or the reason for the withholding of any information. A further exemption exists when information may be withheld in relation to the provision of examination marks before they are officially announced and copies of examination scripts.

### **Processing by the Academy**

Applications will be processed promptly, but in any event a response will be made within one month, as permitted under the Data Protection Act, from the date that the academy accepts the completed application form along with your proof of identity.

We may process a large amount of information about you. To enable us to best deal with requests, we would be grateful if you could clarify the information or processing activities that your request relates to as much as possible. Without further clarification from you regarding the information, it may be possible that we will be unable to respond to requests on the basis that they are manifestly excessive.

### **Proof of identity**

The Academy has a duty to ensure that the information it processes is secure; the Academy will only provide the information relating to you if satisfied regarding your identity, i.e. that you are entitled to the information. The Academy therefore requires you to provide reasonable proof of your identity. Examples of the types of identity documents that will be accepted are listed in the form. Applications that do not include acceptable identity will not be processed, but the Academy will contact you should this be the case.

The Academy does not have to give you any information that might identify any other individual unless that person agrees. If you believe that any information the Academy holds about you may identify another person, you may wish to obtain that person's written consent (to you being given his/her information). That should be submitted to the Academy with this application, along with their proof of identity (to the same standard as is required for yourself).

### **Submission**

When you have completed the form, please send it together with your proof of identity to the Data Protection Officer, The Willow Learning Trust, Glenthorne High School, 270 Sutton Common Road, Sutton, SM3 9PS. Alternatively, the form can be emailed to [DPOfficer@glenthorne.sutton.sch.uk](mailto:DPOfficer@glenthorne.sutton.sch.uk).

## Subject Access Request Form

You can use this form to request access to the personal information held on you/your child by the Willow Learning Trust.

**Please note: The right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf (typically under the age of 13) or has given their consent.**

### Section One – Your Details

Surname:	
First Name(s):	
Previous Surname: (if applicable)	
Address:	
Telephone:	
Email:	
Evidence of identity: (copy of birth certificate, passport, driving licence)	Evidence provided? Yes/No  Details:
Status of Requestor:	Data Subject: Yes/No  Parent or other person with parental responsibility: Yes/No  Other: (please outline your role below)

Please make sure to enclose proof of your identity – such as a photocopy of your passport, driving licence, or birth certificate.

### Section Two – Data Subject's Details (person whose information you are requesting)

Surname:	
Full Name(s):	
Date of Birth:	
Address:	
Year Group (if pupil still at school)	

### Section Three – Your Request

Please provide a description of the data you are requesting in the box below. You may continue overleaf if needed. You should describe the information you need as clearly as possible: it is not sufficient to ask for "everything about me". If your request is too broad or unclear, we may need to ask you to be more specific.

Your request will be handled by our Data Protection Officer who will respond within 28 working days.

### Section Four – Declaration

I hereby request that the Willow Learning Trust provide the data requested about.....(insert name) on the basis of the authority that I have.

Signed : \_\_\_\_\_

Date : \_\_\_\_\_

**Warning – attempting to obtain personal data to which you are not entitled may be an offence under the Data Protection Act.**