Data Protection Policy

Last reviewed: August 2023

This document has been prepared in accordance with the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and other related legislation, and applies to all schools and operations of the Vale Academy Trust.

The following related policies/procedures can be found on Trust/school websites or copies can be obtained from Trust/school offices upon request:

- Data Protection Biometric Data Policy
- Data Protection Privacy Notice for Job Applicants
- Data Protection Privacy Notice for Pupils, Parent and Carers
- Data Protection Privacy Notice for Staff
- Data Protection Photograph Policy
- Data Protection Data Breach Procedure
- Records Retention Policy

Document Control			
Review period	24 Months	Next review	August 2025
Owner	Data Protection Officer	Approver	Board of Directors
Category	Public	Type	Global

INTRODUCTION

1.1. The Vale Academy Trust ("the Trust") collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with its schools and other operations in order to provide education and associated functions. The Trust 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 DPA, the UK GDPR and other related legislation.

1.2. The aim of this policy is to ensure that Trust staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their duties.

1.3. The data protection legislation applies to personal data in computerised form and in manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that makes it searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.4. We will review and update this policy on an annual basis in accordance with our data protection obligations. This policy does not form part of any contract of employment or consultancy agreement and we may amend, update or supplement it from time to time. We will circulate any new or materially modified policy to staff when it is adopted.

2. SCOPE

2.1. This policy applies to all Trust staff. Any reference to the term staff in this policy includes employees, governors / trustees / directors, volunteers, consultants, contractors, interns, temporary workers, visiting music teachers (VMTs), any peripatetic workers and sports coaches, agency workers and casual workers.

2.2. Staff should refer to the Trust's privacy notices and, where appropriate, to other relevant policies including those relating to information security, data retention, bring your own device (BYOD), and personal data breaches, which contain further information regarding the protection of personal data in those contexts.

2.3. All staff are required to read and confirm that they understand this policy.

3. PERSONAL DATA

3.1. 'Personal data' is information that identifies a living individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

3.1.1. race or ethnic origin;

3.1.2. political opinions;

3.1.3. religious or philosophical beliefs;

3.1.4. trade union membership;

3.1.5. physical or mental health;

3.1.6. an individual's sex life or sexual orientation;

3.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

3.2. Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

3.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so. This information includes personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings).

3.4. The Trust does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or students except where the Trust has been notified of the information, or it comes to the Trust'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 Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member 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).

4. THE DATA PROTECTION PRINCIPLES

4.1. When processing personal data, the Trust and its staff must comply with the data protection principles set out in Article 5 of the UK GDPR at all times:

4.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met ('***lawfulness, fairness and transparency'***);

4.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes (***'purpose limitation'***);

4.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed ('***data minimisation'***);

4.1.4. personal data shall be accurate and, where necessary, kept up to date (***'accuracy'***);

4.1.5. personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes (***'storage limitation'***);

4.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (***'integrity and confidentiality'***).

4.2. In addition, the Trust is also responsible for, and be must be able to demonstrate compliance with the above principles ('***accountability'***). This means that the Trust will:

4.2.1. inform individuals about how and why we process their personal data through the privacy notices we issue;

4.2.2. be responsible for checking the quality and accuracy of the information;

4.2.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;

4.2.4. ensure that when information is authorised for disposal it is done appropriately;

4.2.5. 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 times;

4.2.6. share personal information with others only when it is necessary and legally appropriate to do so;

4.2.7. set out clear procedures for responding to requests for access to personal information known as subject access requests;

4.2.8. report any breaches of data protection legislation in accordance with the procedure in paragraph 12 below.

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1. The Trust is responsible for ensuring that personal data is processed in a lawful, fair and transparent way. In relation to any processing activity we will, before the processing begins, and then regularly while it continues:

5.1.1. review the purposes of the particular processing activity, and identify which of the following legal bases for processing (as set out in Article 6 of the UK GDPR) is most appropriate:

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

b) The processing is necessary for the **performance of a contract**, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

c) The processing is necessary for the performance of a **legal obligation** to which we are subject.

d) The processing is necessary to **protect the vital interests of the individual** or another i.e. to protect someone's life.

e) The processing is necessary for the performance of a **task carried out in the public interest**, or in the exercise of **official authority** vested in us.

f) The processing is necessary for the **legitimate interests of the Trust** (where the processing is not for any tasks that the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden by those interests.

5.2. When determining whether the legal basis of legitimate interests is appropriate, we will:

5.2.1. carry out a legitimate interests assessment ("LIA") (a type of light-touch risk assessment) and keep a record of it, to ensure that we can justify our decision;

5.2.2. if the LIA identifies a significant risk to an individual's data protection rights, consider whether we also need to conduct a data protection impact assessment ("DPIA";

5.2.3. keep the LIA under review, and repeat it if circumstances change; and

5.2.4. include information about our legitimate interests in our relevant privacy notice(s).

5.3. Where processing of personal data is likely to result in a high risk to individuals, we will, before commencing the processing, carry out a DPIA to assess:

5.3.1. whether the processing is necessary and proportionate in relation to its purpose;

5.3.2. the risks to individuals; and

5.3.3. what measures can be put in place to address those risks and protect personal information.

5.4. In order to comply with its transparency obligations, the Trust will issue privacy notices from time to time, informing individuals about the personal data that we collect and hold, how they can expect personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6. PURPOSE LIMITATION

6.1. You must not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and, where necessary, they have consented.

7. DATA MINIMISATION

7.1. You may only collect personal data to the extent required for your duties, and should ensure that any personal data collected is adequate and relevant for the intended purposes. In order to do this, you should:

7.1.1. minimise the processing of personal data (for example through redaction) and the deletion of long emails trails;

7.1.2. anonymise personal data where appropriate;

7.1.3. pseudonymise personal data where possible, for example, through the use of initials rather than full names; and

7.1.4. ensure that when personal data is no longer needed, it is deleted.

8. ACCURACY

8.1. Staff have a responsibility for helping the Trust keep their own personal data up to date. You should let the Data Protection Officer know if the information you have provided to the Trust changes, for example if you move house or change details of the bank or building society account to which you are paid. This helps the Trust comply with its wider data protection obligations and can reduce the likelihood of a data breach occurring. The Trust also asks parents to inform them of any changes to their or their child's personal data.

9. STORAGE LIMITATION

9.1. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow guidance contained in the Records Retention Policy, which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

9.2. Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

10. INTEGRITY AND CONFIDENTIALITY

10.1. The Trust will use appropriate technical and organisational measures in accordance with our information security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10.2. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

10.3. All staff have an obligation to report actual or suspected personal data breaches to the Data Protection Officer immediately upon discovery.

11. DOCUMENTATION AND RECORDS

11.1. We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category data or criminal offence data, including:

11.1.1. the purposes of the processing;

11.1.2. a description of the categories of individuals and categories of personal data;

11.1.3. categories of recipients of personal data;

11.1.4. where relevant, details of transfers of personal data outside the UK, including documentation of the transfer mechanism safeguards in place;

11.1.5. where possible, retention schedules; and

11.1.6. where possible, a description of technical and organisational security measures.

11.2. As part of our record of processing activities we document, or link to documentation, on:

11.2.1. information required for privacy notices;

11.2.2. records of consent;

11.2.3. controller-processor contracts;

11.2.4. the location of personal information;

11.2.5. DPIAs; and

11.2.6. records of personal data breaches.

11.3. If we process special category data or criminal offence data, we will keep written records of:

11.3.1. the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

11.3.2. the lawful basis and additional conditions relied upon to process this information; and

11.3.3. whether we retain and erase the personal information in accordance with our Records Retention Policy and, if not, the reasons for not following the Records Retention Policy.

11.4. We will conduct regular reviews of the personal information we process and update our documentation accordingly.

12. INDIVIDUAL OBLIGATIONS

12.1. If you have access to personal data, you must:

12.1.1. only access the personal data that you have authority to access, and only for authorised purposes;

12.1.2. only allow other staff to access personal data if they have appropriate authorisation;

12.1.3. only allow individuals who are not staff to access personal data if you have specific authority to do so from the Data Protection Officer;

12.1.4. keep personal data secure; and

12.1.5. to the extent that you may use personal devices for work purposes, comply with the Trust's BYOD Policy.

13. TRAINING

13.1. The Trust will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

14. WORKING REMOTELY

14.1. As part of our commitment to flexible working, the Trust supports homeworking in appropriate circumstances, either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular basis (full or part-time).

14.2. Working remotely can lead to increased risk in terms of the security of Trust information (including personal data) and communications systems. When working remotely, you must comply with all relevant policies, including our:

14.2.1. Staff Data Protection Policy (this policy);

14.2.2. Information Security Policy;

14.2.3. Records Retention Policy

14.2.4. Staff Code of Conduct

14.2.5. Remote working policy,

at all times and to attend any additional training on data protection and confidentiality as may be required by the Trust.

15. USE OF PERSONAL DATA BY THE TRUST

15.1. The Trust processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles.

Pupils

15.2. 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, and photographs.

15.3. 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 school and the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment.

15.4. The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or carers for fundraising, marketing or promotional purposes and to maintain relationships with pupils, but only where consent has been provided to this.

15.5. In particular, the Trust may:

15.5.1. transfer information to any association, society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained;

15.5.2. make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

15.5.3. use photographs of pupils in accordance with the photograph policy.

15.6. Any wish to limit or object to any use of personal data should be notified to the headteacher of the relevant school in writing, which notice will be acknowledged by the school in writing. If, in the view of the headteacher, the objection cannot be maintained, the individual will be given written reasons why the school cannot comply with their request.

Staff

15.7. The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs for ID purposes, occupational pensions, and other personal data related to employment in the Trust.

15.8. The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

15.9. 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.

15.10. **Disclosure and Barring Service (DBS):** Staff should be aware that DBS checks are carried out on the basis of the Trust's legal obligations in relation to the safer recruitment of staff as stipulated in the Independent School Standards Regulations, and that the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Records Retention Policy which can be found on the Trust website:

Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the Data Protection Act 2018 and the UK GDPR, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

15.11. Any wish to limit or object to the uses to which personal data is to be put should be notified to the appropriate headteacher who will ensure that this is recorded, and adhered to if appropriate. If the headteacher 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 request cannot be complied with.

15.11.1. A staff member whose principal place of work is at the Trust's central operations unit should make their request to their line manager or the Chief Executive.

Other Individuals

15.12. The Trust may hold personal information in relation to other individuals who have contact with the school, 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.

16. SECURITY OF PERSONAL DATA

16.1. The Trust 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 data protection legislation. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

16.2. For further details as regards security of IT systems, please refer to the ICT Policy.

17. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

17.1. The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

17.1.1. To give a confidential reference relating to a current or former employee, volunteer or pupil;

17.1.2. for the prevention or detection of crime;

17.1.3. for the assessment of any tax or duty;

17.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);

17.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

17.1.6. for the purpose of obtaining legal advice;

17.1.7. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

17.1.8. to publish the results of public examinations or other achievements of pupils of the Trust;

17.1.9. to disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips; the legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals);

17.1.10. to provide information to another educational establishment to which a pupil is transferring;

17.1.11. to provide information to Examination Authorities as part of the examination process;

17.1.12. to provide information to the Department for Education (DfE). Examination Authorities may also pass information to the DfE and

17.1.13. to provide information to the emergency services and local authorities to help them respond to an emergency situation that affects any of our pupils or staff

17.2. 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.

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

17.4. If you require guidance on release of personal data to third parties, you should contact the Trust's Information Team, using the contact details below.

Email: InformationTeam@vale-academy.org

Or you can send a letter addressed to:

Information Team
Vale Academy Trust
The Studio, St Mary's Convent
Denchworth Road
Wantage
OX12 9AU

18. CONFIDENTIALITY OF PUPIL CONCERNS

18.1. Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or carer, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest. Further information on safeguarding can be found in the Safeguarding and Child Protection Policy, which can be found on the Trust website

19. SUBJECT ACCESS REQUESTS

19.1. Anybody who makes a request to see any personal information held about them by the Trust is making a Subject Access Request. 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" (see para 1.2).

19.2. The individual's full subject access right is to know:

- whether personal data about him or her are being processed
- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom their personal data have been or will be disclosed

- the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored
- the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- the right to lodge a complaint with the Information Commissioner's Office
- Where the personal data are not collected from the individual, any available information as to their source
- Details of the safeguards in place for any transfers of their data to locations outside the UK.

19.3. If you, as a member of staff, receive a SAR from a pupil, parent or carer or other person, you should immediately forward it to the Data Protection Officer.

19.4. If you require guidance on how to handle a Subject Access Requests, you should contact the Trust's Information Team using the contact details under para 17.4above.

19.5. The Trust will always seek to respond in full to Subject Access Requests within one month of receipt, although this may be difficult to achieve when schools are closed for holidays, particularly in the summer (and subject to the rights of the Trust to extend the time limit for response by a further two months, considering the complexity and number of the requests, in accordance with Article 12(3) of the UK GDPR).

19.6. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Trust must, however, be satisfied that:

19.6.1. the child or young person lacks sufficient understanding; and

19.6.2. the request made on behalf of the child or young person is in their interests.

19.7. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the Trust must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

19.8. 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 into any alleged offence(s).

19.9. The Trust must decide whether to apply any potential exemption (taking legal advice where appropriate), based on the circumstances of a particular request.

19.10. A subject access request may be made verbally or in writing. Where possible, the Trust prefers requests to be made in writing. The Trust may ask the data subject for any further information reasonably required to locate the information.

19.11. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

19.12. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

19.13. All records must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by the Data Protection Officer. Any disclosure can only take place after the response is approved by the Data Protection Officer. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the supplementary information the requestor is entitled to (please see para 19.2).

20. OTHER RIGHTS OF INDIVIDUALS

20.1. The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

20.1.1. object to Processing;

20.1.2. rectification;

20.1.3. erasure; and

20.1.4. data Portability.

Right to object to processing

20.2. Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purposes. This right is absolute and where such an objection is made the Trust will stop processing personal data for this purpose.

20.3. An individual also has the right to object to the processing of their personal data on the legal basis of:

20.3.1. a task carried out in the public interest;

20.3.2. the exercise of official authority vested in the Trust; or

20.3.3. the legitimate interests of the Trust or a third party.

20.4. Where such an objection is made, it must be sent to the Data Protection Officer immediately. They will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the

information is required for the establishment, exercise or defence of legal proceedings.

20.5. The Data Protection Officer is responsible for notifying the individual of the outcome of their assessment without undue delay and within one calendar month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR). If the request is refused, the response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

Right to rectification

20.6. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to The Information Team, using the contact details under para 7.4 above, and where adequate proof of inaccuracy is given, the data shall be amended without undue delay and in any case within one calendar month, and the individual notified.

20.7. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review by a senior member of Trust staff and information on how to complain using the Trust's complaints policy, and how to appeal directly to the ICO.

20.8. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way, once verified, shall be updated without undue delay.

20.9. Where a request is refused, the request and reasons for refusal shall be documented and notice of refusal should be provided to the individual within a month of receipt of the request. The Trust will include in its response the reasons why the request has been refused and information about the individual's right to complain to the ICO and to bring a civil claim.

20.10.

Right to erasure

20.11. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

20.11.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

20.11.2. where consent is withdrawn and there is no other legal basis for the processing;

20.11.3. where an objection has been raised under the right to object, and found to be legitimate;

20.11.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

20.11.5. where there is a legal obligation on the Trust to delete or otherwise destroy.

20.12. The Data Protection Officer will make a decision 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.

20.13. Where a request is refused, the Trust will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

Right to restrict processing

20.14. In the following circumstances, processing of an individual's personal data may be restricted:

20.14.1. where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;

20.14.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

20.14.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

20.14.4. where there has been an objection made pending the outcome of any decision.

Right to portability

20.15. If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If such a request for this is made, it should be forwarded to the Data Protection Officer immediately and this will be reviewed and actioned as necessary.

21. BREACH OF ANY REQUIREMENT OF DATA PROTECTION LEGISLATION

21.1. Any and all breaches of data protection legislation, including a breach of any of the data protection principles, shall be reported **as soon as it is/ they are discovered** to the Information Team using contact details in 17.4 above

21.2. Once notified, the Information Team shall assess:

21.2.1. the extent of the breach;

21.2.2. the risks to the data subjects as a consequence of the breach;

21.2.3. any security measures in place that will protect the information;

21.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

21.3. Unless the Information Team concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

21.4. The Information Commissioner shall be told:

21.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

21.4.2. the contact point for any enquiries (which shall usually be the Data Protection Officer, who can be contacted using the details under para 7.4 above);

21.4.3. the likely consequences of the breach;

21.4.4. measures proposed or already taken to address the breach.

21.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Officer 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.

21.6. Data subjects shall be told

21.6.1. the nature of the breach;

21.6.2. who to contact with any questions;

21.6.3. measures taken to mitigate any risks.

21.7. The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust's Board of Directors and a decision made about implementation of those recommendations.

22. CONSEQUENCES OF FAILING TO COMPLY

22.1. The Trust takes compliance with this policy very seriously. Failure to comply with the policy:

22.1.1. puts at risk the individuals whose personal information is being processed; and

22.1.2. carries the risk of significant sanctions for the individual staff member and the Trust; and

22.1.3. may, in some circumstances, amount to a criminal offence by the individual staff member.

22.2. Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of your working relationship with the Trust.

23. CONTACT

23.1. If you have any concerns or questions in relation to this policy please contact the Information Team, using the contact details under para 17.4 above.

End of Document