# OWLS Academy Trust

# Data Protection Policy

Date Detail June 25th, 2018

Original, based on Trust Policy 25.06.17

Reviewed annually

Approved by Jonathan Tedds, Chair of Governor

| | |
|---|---|
| Adopted by The OWLS Academy Trust on | |
| Next Review Due | Reviewed Annually in May |

The OWLS Academy Trust recognises that every 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 schools within the OWLS Academy Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially children's services.

This policy aims to ensure that all staff, governors and trustees are aware of their responsibilities and outlines how the Trust and its member schools comply with the requirements of the GDPR.

This policy does not form part of any employee's contract of employment and may be amended at any time.

## Legal Framework

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

- The General Data Protection Regulation (GDPR) (2016)
- 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 published by the Information Commissioner's Office:

- "Overview of the General Data Protection Regulation (GDPR)" (2017)
- "Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now" (2017)

This policy will be implemented in conjunction with other Trust policies and procedures, including, but not limited to:

- Expectable use-security Policy
- Freedom of Information Policy

## Definitions

**"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection; recording; organisation; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission, dissemination or otherwise making available; alignment or combination; restriction; erasure; or destruction.

**"Personal data"** means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**"Special Categories of Personal Data"** means sensitive personal data and includes genetic data, biometric data, health data and data relating to a person's race, ethnicity, religious/political beliefs and sexual orientation. Additional criteria must be met if Special Category Personal Data is to be processed.

**"Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

## Data Protection Principles

We will comply with the six principles relating to the processing of personal data as set out in the GDPR, which requires that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- 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;
- Retained only for as long as necessary; and
- Processed in an appropriate manner to maintain security;

## Accountability

The Trust will ensure that appropriate technical and organisational measures are put in place across all schools to demonstrate that data is processed in line with the principles set out in the GDPR.

The Trust will produce comprehensive, clear and transparent template privacy statements in respect of data processing activities that are common to all schools. Each school will then be required to check that these meet and address all of their data processing requirements – where any gaps are identified they must ensure that these are addressed promptly.

Additional internal records of each school's processing activities will be maintained and kept up-to-date, and will include:

- Name and details of the organisation and school;
- 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 Trust, and each member school, will implement measures that meet the principles of data protection by design and by default, such as:

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

Data protection impact assessments (DPIAs) will be used where appropriate.

## Data Protection Officer (DPO)

The Trust has appointed a School Business Manager to the role of DPO for the Trust, and will ensure that there is no conflict of interest in their duties. The DPO has suitable skills, knowledge, experience and/or qualification in order to fulfil the requirements of this role, which is to:

- Inform and advise the Trust , its member schools and their employees about their obligations to comply with the GDPR and other data protection laws;
- Monitor GPPR compliance across the entire Trust, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing training to staff members.

The DPO reports to the highest level of management within the Trust, specifically to the CEO and Chair of Trustees, but is able to operate independently in order to fulfil their duties and will not be dismissed or penalised for performing their task.

## Lawful Processing

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

The processing of personal data will only be lawful if ONE of the following conditions is met:

- The data subject gives consent for one or more specific purposes;
- The processing is necessary for compliance with a legal obligation;
- The processing is necessary for the performance of a contract with the data subject, or to take steps to enter into a contract;
- The processing is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the controller;
- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing is 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. (Note that this condition is not available to data processing undertaken by a school in the performance of its tasks.)

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

We will only process “special categories of personal data” (data about race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, health, genetic data, biometric data, sex life, sexual orientation) where there is a legal basis for processing the data (as above) and at least one of the following conditions are also met:

- The data subject has given explicit consent (unless reliance on consent is prohibited by EU or UK law);
- Processing related 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;
- Processing is necessary to protect the vital interests of the data subject or another individual where the data subject is physically or legally incapable of giving consent;
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Reasons of public interest in the area of public health;
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment of management of health or social care systems and services, on the basis of EU or UK law or a contract with a health professional;
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

## Consent

Consent will be sought prior to processing any data which cannot be processed 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, and 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.

Consent can be withdrawn by the individual at any time. Where consent is withdrawn the data processing activity will be stopped with immediate effect.

The Trust and its member schools will ensure that consent mechanisms meet the standards of the GDPR: where the standard of consent cannot be met then an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the Data Protection Act (DPA) will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

Where consent is required for data processing in respect of a child under the age of 13, the consent of parents will be sought prior to the processing of the 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 metal 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.

## Rights of Data Subjects

### The Right to be Informed

Privacy notices will be supplied to individuals in regards to the processing of their personal data, and 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/Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

The following information will be supplied within all privacy notices:

- The contact details of the controller (the School or the Trust) and, where applicable, the controller's representative;
- The contact details of the Data Protection Officer;
- The purpose(s) and legal basis for processing the data;
- The legitimate interests of the controller or third party;
- The recipients or categories of recipients of the personal data, if any;
- Whether there is any intention to transfer the personal data outside of the EU, and if so the safeguards (adequacy conditions) that are in place;
- The retention period for the data, or the criteria used to determine the retention period;
- The data subjects rights, including the right to:
    - Withdraw consent at any time (where the lawful basis for processing is consent);
    - Rectification, erasure, restriction, objection;
    - 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 anticipated consequences for the data subject.

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 supplied at the time the data is obtained.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the School/Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources will be supplied:

- Within one month of having obtained the data;
- If disclosure to another recipient is envisaged, then before the data are disclosed;
- If the data are used to communicate with the individual, then not later than when the first communication takes place.

## The Right of Access

Individuals have the right to obtain confirmation that their data is being processed, and 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/Trust will verify the identity of the person making the request before any information is supplied.

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

A copy of the information will be supplied to the individual free of charge; however, the Trust 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 then a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

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

All requests will be responded to without delay (within 30 days) and at the latest within one month of receipt. In the event of numerous or complex requests, the period for compliance will be extended by a further 2 months. The individual will be informed of this extension and the reason why it is necessary within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Trust 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 (normally the Information Commissioner's Office) and to a judicial remedy, within one month of the refusal.

### The Right to Rectification

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

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

Where the personal data in question has been disclosed to third parties, the School/Trust will inform them of the rectification where possible. Where appropriate, the individual will be informed about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, the School/Trust 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 its continuing processing, and specifically in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- Where 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/Trust 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.

If personal data has been made public within an online environment, the School/Trust 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 personal data will be stored but will not be further processed, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The processing of personal data will be restricted in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the accuracy of the data has been verified;
- Where an individual has objected to the processing, and the School/Trust is considering whether there legitimate grounds override those of the individual;
- Where processing is unlawful and the individual opposes erasure and requests restriction instead;
- Where the personal data is no longer needed by the School/Trust 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/Trust 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/Trust 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. The right to data portability only applies in cases where:

- The personal data has been provided by an individual to a controller;
- The processing is based on the individual's consent or for the performance of a contract; AND
- Processing is carried out by automated means.

Personal data will be provided free of charge in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Schools are 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, consideration will be given as to whether providing the information would prejudice the rights of any other individual.

The school/Trust will respond to any requests for portability within one month. However, where the request is complex, or a number of requests have been received, the timeframe can be extended by 2 months. Where an extension is necessary, the individual will be 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, then without delay and at the latest within one month the individual will be informed of the reasons for this and of their right to complain to the supervisory authority and to a judicial remedy.

### The Right to Object

The School/Trust 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:

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

Where personal data is processed on the grounds of legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation;
- The School/Trust 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/Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Direct marketing is not generally undertaken by or on behalf of the Trust or its member schools. However, should such processing be undertaken then the School/Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes, and therefore will stop processing personal data for direct marketing as soon as an objection is received.

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/Trust 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/Trust will offer a method for individual's 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) and it produces a legal or similarly significant effect on the individual.

The School/Trust 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/Trust will ensure that 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/Trust has the explicit consent of the individual; or
- The processing is necessary for reasons of substantial public interest on the basis of EU or UK law.

## Privacy by Design and Privacy Impact Assessments

The Trust and its member schools will act in accordance with the GDPR by adopting a privacy by design approach and by implementing technical and organisational measures which demonstrate how they have considered and integrated data protection into processing activities.

Data Protection Impact Assessments (DPIAs) enable the identification and resolution of problems at an early stage, and will be used to identify the most effective method of complying with data protection obligations and meeting individual's expectations of privacy.

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:

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

All DPIAs will include, as minimum, 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 Data Protection Officer will consult the Information Commissioner's Office (ICO) to seek its opinion as to whether the processing operation complies with the GDPR.

## Data Breaches

The term "personal data breach" refers to a breach of security which has led to the destruction; loss; alteration; or unauthorised disclosure of, or access to, personal data. The Head Teachers will ensure that all staff members within their school are made aware of and understand what constitutes a data breach, and will then remind all staff on a regular basis.

Where a breach is likely to result in a risk to the rights and freedoms of individuals the relevant supervisory authority (currently the Information Commissioner's Office) will be notified within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis by the DPO and/or School Business Manager.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly. A "high risk" breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at all schools across the Trust, which facilitate decision-making in relation to whether the supervisory authority or the public need to be notified.

With 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; and
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

## Data Security

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access. When in use confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected. Where data is saved on removable storage or a portable device, the device will be fully encrypted. Where data is saved on a network drive it will be regularly backed up off-site and network access will be subject to individual secure login and regularly updated password.

All electronic devices are password-protected to protect the information on the device in case of theft. In addition, where possible the schools enable electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not store any school-related personal data on their personal laptops or computers, with the exception of their school e-mail account (including contacts) which may be linked to their personal mobile phone provided that this is locked at all times when not in use.

E-mails containing sensitive or confidential information are pass-word protected if there are, or may be, unsecure servers between the sender and the recipient.

Circular e-mails to parents must be sent blind carbon copy (bcc) so e-mail addresses are not disclosed to other recipients.

Confidential information should only be sent by fax if there is no alternative, and then only after the school has checked the fax number is correct and the recipient is standing by to receive the information.

Where personal information is taken off the school premises, whether in electronic or paper format, staff will take extra care to ensure the security of the data (e.g. keeping data under lock and key, use of robust data encryption, etc). The personal data to be taken from the school premises must be kept to the minimum necessary and the person taking it must accept full responsibility for the security of the data.

Before sharing any personal data, staff members must ensure that:

- They are allowed to share it with the intended recipient;
- Adequate security is in place to protect it;
- The recipient of the data has been outlined in a privacy notice.

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

The physical security of all school buildings and storage systems within the Trust, and access to them, is reviewed regularly. If an increased risk in vandalism/burglary/theft is identified, extra measures will be put in place to secure data storage.

The Head Teacher has overall responsibility for ensuring that continuity and recovery measures are in place for the security of protected data.

The OWLS Academy Trust takes its duties under the GDPR seriously and any unauthorised disclosure of personal data may result in disciplinary action.

## Publication of Information

Academies and Academy Trusts are required, by law, to publish certain information on their school website and these documents include names of some staff, governors and trustees. Such information will be kept to the minimum level needed for legal compliance. Photos will never be posted on websites unless the affected individual has given their explicit consent.

Other information must be routinely available on request, including minutes of governor /trustee meetings. Use of personal data will therefore be kept to a minimum, and where possible and appropriate will be pseudonymised or anonymised.

## CCTV and Photography

The Trust recognises that recording images of identifiable individuals constitutes processing personal information.

### CCTV

Where CCTV is used, notices will be clearly displayed to inform people of this, and cameras will only be placed where they do not intrude on anyone's privacy and are necessary to fulfil the intended purpose.

CCTV footage will be deleted after 28 days, except where specific images must be retained for longer as evidence relating to a specific incident.

### Photography and Video Images

Photography and video images are useful tools for teaching and learning, assessment and display purposes. In addition, anonymous use of photographs in publications such as school prospectus and newsletters and on the school website helps to promote the school to interested parties.

The schools will always indicate their intentions for taking photographs / videos and will obtain explicit consent from the individual or, in the case of images of pupils from their parent/legal guardian.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use are exempt from the GDPR. Schools will always remind parents attending events that photographs/videos featuring any child other than their own must never be shared, particularly on social media.

## Data Retention

Personal data will not be kept for longer than is necessary; unrequired data will be deleted as soon as practicable. The Trust has developed a data retention schedule which sets out recommended retention periods, and data should only be held for longer than the timescales set out in this document where there is objective justification to do so.

Some educational records relating to former pupils or employees of the school may be retained for an extended period for legal reasons, but also to enable the provision of references.

Paper documents will be shredded or pulped and electronic memories scrubbed clean or destroyed once the data should no longer be retained.