OVERTON GRANGE SCHOOL
POLICY

DATA PROTECTION

Govs Comm. FULL GOVERNING BODY

Reasons for the policy

Overton Grange School collects and uses certain types of personal information about staff, students, parents/carers and other individuals who come into contact with the school in order provide education and associated functions. The school 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 UK General Data Protection Regulation (GDPR) and other related legislation.

The GDPR applies to all computerised data and 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 it is 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.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every two years.

This policy meets the requirements of the

- UK General Data Protection Regulation (GDPR)
- Data Protection Action 2018 (DPA)
- Regulation 5 of the Education (Pupil Information) (England) Regulations 2005

It also reflects the ICOs guidance for the use of surveillance cameras and personal information

How the policy is going to be put into practice

PERSONAL DATA

Personal data is information that identifies an 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]. Personal data may include the individual's:

- Name (including initials)
- Identification number, e.g. URN/ULN
- Location data

[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.

- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sexual life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person.

Special Category personal data is more sensitive and, as such, 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 school does not intend to seek or hold sensitive personal data about staff or students except where the school has been notified of the information, or it comes to the school'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 school 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).

THE DATA PROTECTION PRINCIPLES

The six data protection principles as laid down in the GDPR are followed at all times:

- 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;
- Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- 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.

In addition to this, the school is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail below).

The school is committed to complying with the data protection principles at all times. This means that the school will:

- only collect personal data for specified, explicit and legitimate reasons.
- 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. Inaccurate data will be rectified or erased when appropriate;
- 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 Records Retention procedure [See Appendix 1];
- 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 times;
- 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.

CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

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

1 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.

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

3 The processing is necessary to protect the vital interests of the individual or another.

4 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.

5 The processing is necessary for a legitimate interest of the school or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

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

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
- The processing is necessary to protect the vital interests of the individual or another, where the individual is physically or legally incapable of giving consent.
- The processing is necessary for the performance of or to exercise obligations or right in relation to employment, social security or social protection law.
- The data has already been made manifestly public by the individual.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest as defined in legislation.
- The processing is necessary for health and social care purposes and is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The processing is necessary for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The processing is necessary for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law.

USE OF PERSONAL DATA BY THE SCHOOL

The school holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined above.

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

Students

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

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

In particular, the school may:

- Transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the school but only where consent has been obtained first

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

- Use photographs of students in accordance with the Child Media Policy.

Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs, other relevant professional information.

The data is used to comply with legal obligations placed on the school in relation to employment, and the education of children in a school environment. The school 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.

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.

Data may be used for regular school administration and also for statutory returns.

Other Individuals

The school 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.

SECURITY OF PERSONAL DATA

The school 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 school will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. This will include, but is not exclusive to:

- Keeping paper-based records under lock and key when not in use
- Ensuring that papers containing confidential personal data are not left on office or classroom desks, on staffroom tables, or left anywhere else where there is general access
- Using encryption software to protect all portable devices and removable media, such as USB devices

Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.

For further details as regards security of IT systems, please refer to the Network Manager.

DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

Where the school needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected. Where we transfer person data internationally, we will do so in accordance with UK data protection law.

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

- to give a reference relating to a current or former employee, volunteer or student;
- for the prevention or detection of 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 school (other than an obligation imposed by contract);
- for the purpose of, 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 damage or distress);
- to publish the results of public examinations or other achievements of students of the school;
- to disclose details of a student's medical condition where it is in the student's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

- to provide information to another educational establishment to which a student is transferring;
- to provide information to the Examination Authority as part of the examination process;

- to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE; and

- other disclosures that would be reasonable but not breaching GDPR principles.

The DfE uses information about students 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 students 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 school may receive requests from third parties (i.e. those other than the data subject, the school, and employees of the school) to disclose personal data it holds about students, 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 school.

All requests for the disclosure of personal data must be sent to the Headteacher (or their nominated representative), 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.

CONFIDENTIALITY OF STUDENT CONCERNS

Staff are expected to follow the school's Child Protection Policy and Procedures, which does not allow them to promise confidentiality to students. However, where a student seeks to raise concerns with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or carers, the school will maintain this confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the school believes disclosure will be in the best interests of the student or other students. Any queries relating to this matter should be referred to the school's Designated Safeguarding Lead.

SUBJECT ACCESS REQUESTS

Anybody who makes a request to see any personal information held about them by the school 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".

All requests should be sent to the Headteacher (or their nominated representative) within two working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt or, if complex or if there are issues with staff availability, within a maximum of three months.

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 Headteacher (or their nominated representative) 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 own information rights, may appoint another person to request access to their records. In such circumstances the school must have written evidence that the individual has authorised the person to make the application and the Headteacher (or their nominated representative) must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

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

A subject access request must be made in writing. The school may ask for any further information reasonably required to locate the information.

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.

All files must be reviewed by the Headteacher (or their nominated representative) before any disclosure takes place. Access will not be granted before this review has taken place.

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

Exemptions to access by data subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If the school intends to apply any of them to a request, then we will usually explain which exemption is being applied and why.

There is no automatic parental right of access to the education record of children in Academies. Details of the school's approach to parental requests can be found in Appendix 2: Student Records.

OTHER RIGHTS OF INDIVIDUALS

The school 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 school will comply with the rights to:

a. object to processing;
b. rectification;
c. erasure;
d. right to restrict processing; and
e. data Portability.

a. Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (Data principles 4 and 5, page 4 above) where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the Headteacher (or their nominated representative) within two working days of receipt, and the Headteacher (or their nominated representative) will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The Headteacher (or their nominated representative) shall be responsible for notifying the individual of the outcome of their assessment within ten working days of receipt of the objection.

b. Right to rectification

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 Headteacher (or their nominated representative) within two working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

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 bringing a complaint / grievance under the usual procedure, or an appeal direct to the Information Commissioner.

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

c. Right to erasure

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

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- where consent is withdrawn and there is no other legal basis for the processing;
- where an objection has been raised under the right to object, and found to be legitimate;
- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- where there is a legal obligation on the school to delete.

The Headteacher (or their nominated representative) 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.

d. Right to restrict processing

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

- where the accuracy of data has been contested, during the period when the school is attempting to verify the accuracy of the data;
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- 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;
- where there has been an objection made under point 2 in 'Right to erasure' above, pending the outcome of any decision.

e. Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that the school provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the school 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 a request for this is made, it should be forwarded to the Headteacher (or their nominated representative) within two working days of receipt, and the Headteacher (or their nominated representative) will review and revert as necessary.

CCTV

The school uses CCTV in various locations around the school site to ensure it remains safe. The school follows the ICOs guidance for the use of CCTV, and complies with data protection principles.

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

Any enquiries regarding the CCTV system should be directed to the Network Manager.

BREACH OF ANY REQUIREMENT OF THE GDPR

Any and all breaches, or potential breaches, of the GDPR, including a breach of any of the data protection principles must be reported as soon as it is discovered, to the Headteacher (or their nominated representative) and on GDPRiS[2].

Once notified, the Headteacher (or their nominated representative) 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;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Headteacher (or their nominated representative) concludes that there is unlikely to be any risk to individuals from the breach (using the ICO Self-Assessment tool where necessary), it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the school, unless a delay can be justified.

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries, which shall usually be the Headteacher (or their nominated representative);
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

[2] GDPR in Schools (GDPRiS) is a cloud-based, data protection monitoring system. It allows us to carry out SARS, to track, monitor and manage incidents and breaches in accordance with ICO requirements, and provides us with an independent DPO.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Headteacher (or their nominated representative) 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.

Data subjects shall be told:

- the nature of the breach;

- who to contact with any questions;
- measures taken to mitigate any risks.

The Headteacher (or their nominated representative) shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations from the DPO or ICO for further training or a change in procedure shall be reviewed by the Headteacher and, where necessary, the governing body and a decision made about implementation of those recommendations.

RETENTION OF RECORDS AND STUDENT RECORDS

In order to comply with the principles of this Data Protection Policy, the school has specific rules on the retention of data and specific rules on the use of student records. These rules are appended to this policy.

TRAINING

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

Data protection will form a part of whole-school CPD as necessary, such as when legislation, guidance or school processes are updated.

Roles and responsibilities

The school processes personal data relating to staff, students, parents/carers, governors, visitors and others, and therefore is a data controller. The school is registered with the ICO, as legally required.

- All staff are responsible for collecting, storing and processing any personal data in accordance of this policy, and informing the school of any changes to their personal data, such as change of address.

- The Headteacher (or their nominated representative) acts as the representative of the data controller on a day-to-day basis.

- The Governing Body has overall responsibility for ensuring the school complies with all relevant data protection obligations.

- The Data Protection Officer will assist the school to monitor internal compliance, and inform and advise the school on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner.

Our DPO is Tony Sheppard and is contactable via dpois@gdpr.school

Criteria for success

- All personal data collected about staff, students, parents/carers, governors, visitors and others is collected, stored and processed in accordance with UK data protection law.

- Breaches of data protection are minimal and any breaches are reported according to this policy.

Monitoring and evaluation

- This policy will be regularly reviewed by SLT and Governors

Links with other policies

- Biometric Data
- Child Media
- Child Protection
- Equal Opportunities
- Freedom of Information
- Staff ICT Acceptable Use