|  |
| --- |
| Waseley Hills High School |
| DATA PROTECTION POLICY |

**Responsibility: Assistant Headteacher**

**Author: Mr A W Roll**

**Date of Issue: Autumn 2019**

**Review Date: Autumn 2021**

**Reference:** WHHS0003

The contents of this policy are reviewed and monitored on a regular basis by Senior Leaders, Heads of Subject and staff with responsibility to that area.

Direct responsibilities are written into job descriptions.



For Approval by FGB July 19

**DATA PROTECTION POLICY - General Data Protection Regulation**

Waseley Hills HighSchool collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner’s Office (ICO) detailing the information held and its use. These details are then available on the ICO’s website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

**Purpose**

This policy is intended to ensure that personal information is dealt with correctly, securely and in accordance with the General Data Protection Regulations (GDPR) 2016, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data must be aware of their duties and responsibilities by adhering to these guidelines.

A full copy of the General Data Protection Regulations (GDPR) 2016) can be found at

<http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>

Further guidance can be found on the Information Commissioners website, <https://ico.org.uk/>

**Terminology**

|  |  |
| --- | --- |
| Data Subject | The identified or identifiable living individual to whom personal data relates. |
| Data Controller | ‘Controller’ means the natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data; This is Waseley Hills High School |
| Data Processor | ‘Processor’ means the natural or legal person which processes personal data on behalf of the controller. |
| Personal Data | Any information relating to an identified or identifiable living individual. |
| Sensitive data | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. |
| Subject Access Request | The Data Subject or their representative has the right to request a copy of the information that is held about them. This is called a Subject Access Request. |
| ICO | The Information Commissioner is the UK’s national supervisory authority for the purposes of the GDPR |
| Identifiable living person | A living individual who can be identified, directly or indirectly, in particular by reference to:  • an identifier such as a name, an identification number, location data or an online identifier; or  • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual. |
| Processing | In relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as:  • collection, recording, organisation, structuring or storage;  • adaptation or alteration;  • retrieval, consultation or use;  • disclosure by transmission, dissemination or otherwise making available;  • alignment or combination; or  • restriction, erasure or destruction |
| Age of Consent | Under the GDPR, the default age at which a person is no longer considered a child is 16, but it allows member states to adjust that limit to anywhere between 13 and 16. The UK will apply a lower age limit for gaining valid consent from children when offering an information society service. In the UK consent will be valid from children of at least 13 years old. |
| **Privacy notices for children** | Where services are offered directly to a child, data controllers must make sure that privacy notices are written in a clear, plain way that a child will understand. Although the Regulation calls for similar rules about clear language in general, it’s important that data controllers know the age of the intended audience and provide an appropriately phrased notice. |
| Data Protection Officer | The person responsible for ensuring that the GDPR regulations are applied correctly at Waseley Hills High School. All enquiries, both internal and external about GDPR regulations should be forwarded to the DPO. |

**Registration with the ICO**

The designated Data Protection Officer at Waseley is Mr N Baker, but under GDPR all staff have a responsibility to treat student/staff contact information in a confidential manner and follow the guidelines as set out in this document.

* It is the Data Protection Officer’s (DPO) responsibility to ensure that Waseley Hills High School is registered with the ICO as a Data Controller. THE DPO will also be responsible for ensuring that the required fee is paid and registrations are kept up to date. Details are available from the ICO:

<https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/>

* Any changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.
* Breaches of personal or sensitive data shall be notified by the DPO within 72 hours to the Data Subject(s) concerned and the ICO.

**THE DATA PROTECTION PRINCIPLES**

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

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;
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;
3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
4. personal data shall be accurate and, where necessary, kept up to date;
5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
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.

**Legal basis for processing data:**

Under Article 6 of The GDPR, Waseley Hills High School’s needs to state its legal basis for processing data. Our legal bases are as follows –

**(a) Consent:** the member of staff/student/parent has given clear consent for the School to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for the member of staff’s employment contract or student placement contract.

**(c) Legal obligation:** the processing is necessary for the school to comply with the law (not including contractual obligations)

(**d) Public Task:** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

**Conditions for consent**

1. Where processing is based on consent, for example taking and using photographs, the controller needs to be able to demonstrate that the data subject has consented to processing of his or her personal data in writing.

2. The written declaration of consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time in writing. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

**Staff Training**

The School is also committed to ensuring that their staff is aware of data protection policies, legal requirements and adequate training is provided to them. The requirements of this policy are mandatory for all staff employed by the School and any third party contracted to provide services within the school.

**Personal and Sensitive Data:**

All data within the School’s control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

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. 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 sex life or sexual orientation;
* genetic or biometric data for the purpose of uniquely identifying a natural person.

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

The definitions of personal and sensitive data shall be as those published by the ICO

for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the GDPR shall be applied to all personal data processed:

1. **Personal data shall be:**
2. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
3. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
4. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
5. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
6. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
7. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Use of personal data**

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

**Pupils**

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.

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 academy as a whole is doing, together with any other uses normally associated with this provision in a school environment.

**Staff**

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

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.

**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.

**Disclosure of personal data to third parties**

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

* to give a confidential reference relating to a current or former employee, volunteer or pupil;
* for the prevention or detection of crime;
* For the assessment of any tax or duty
* for the purpose of obtaining legal advice;
* to publish the results of public examinations or other achievements
* to disclose details of a pupil’s medical condition where it is in the pupil’s interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
* to provide information to another educational establishment to which a pupil is transferring;
* to provide information to the Examination Authority as part of the examination process;
* to provide information to Department for Education (DfE) & other local authorities
* to provide information to local authorities as necessary, Worcestershire for school cohort and for LAC students, other local authorities

**Fair Processing / Privacy Notice:**

The School shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual’s data. The main premise being that we will be processing data in the way that people would reasonably expect a school to do so in our role of educating students.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as ‘Children’ under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-

and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual’s data shall first be notified to them.

Under no circumstances will the school disclose information or data:

* + that would cause serious harm to the child or anyone else’s physical or mental health or condition
  + indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
  + recorded by the pupil in an examination
  + that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person’s name or identifying details are removed

**Data Security:**

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.

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual’s privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-

assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

**Data Sharing**

Data transferred electronically will either be encrypted or the file will be password protected. Where the data being transferred is in a password protected file, the password will be sent using a separate email.

Personal data about pupils will not be disclosed to third parties without the consent of the child’s parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

• **Other schools**

If a pupil transfers from Waseley Hills High School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child’s academic progress as a result of the move.

• **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external examination bodies.

• **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

• **Right to be Forgotten:**

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

**Photographs and Video:**

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. Prior consent will be in writing and each proposed use will be covered by separate consent.

**Location of information and data:**

Hard copy data, records, and personal information must be stored out of sight and in a locked cupboard or filing cabinet. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances. A record of what has been taken and when it has been returned should be kept.

• Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers. The Print to Photocopier function should be used so that personal and sensitive data is only printed when a member of staff is at the copier.

• If it is necessary to transport data away from school for exceptional reasons such as for SEN students or safeguarding reasons, it should be downloaded onto an encrypted USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. As soon as possible work should be saved on the school system and the data on the USB erased.

• USB drives on all staff machines have been blocked to prevent saving of data to these devices.

These guidelines are to be clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

**Use of Computers**

* Password should be “strong” password, consisting of a minimum of 8 characters included at least one of;
  + Upper case
  + Lower case
  + Number
  + Special character
* Passwords should not be shared
* They should be changed at least monthly. If a user suspects that some-one else knows there password, it should be changed immediately.
* If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. No machine should be left logged on, the “lock “function should always be used when temporarily leaving a machine if it cannot be logged off. Personal data should not be viewed on public computers.
* No personal information should be viewable from the public area. If there is a risk of this, a privacy screen should be used.
* Personal data such as registers should not be projected in the classroom
* Emails should only be addressed to those who need to know and attention needs to be given to email distribution lists.

**Job related network access rights**

The school will ensure that staff and students will only be able to view data that is necessary for them to carry out their role. Each staff role will be reviewed to ensure that where it is unnecessary for an employee to see certain data they are not allowed to. For example staff contact details will not be available for all to see.

Where appropriate staff may be given read only rights as opposed to edit/write permissions to help maintain data integrity.

**Review of Teaching Activities**

* Students’ mark, attendance details, positive and negatives rewards should not be projected, displayed or called out by the teacher. This is not an exhaustive list and should include all personal data.
* Planners and Progress files should not be left out and should be kept in lockable drawers.
* Parents need to be identified before data is shared with them
* Trip paperwork has to include emergency contact deals and medical information. This has to be taken out of school on paper in case of an emergency. Staff who have this need to ensure that it is securely maintained at all times and returned to the school office at the earliest possible point.

**Backup of School MIS Data, Student and Staff files**

All data is backed up every night to the MS Block to ensure that a complete copy of the data is held in a different building. The MIS system backup files are zipped before being backed up.

**Security of Computer Network**

Access to the computer network is via a user name and password. The MIS system is protected on 2nd level as separate user name and password is required and students’ accounts do not have access to the MIS server. Access to specific areas of the MIS is governed by role based user privileges.

Parental and staff access to the MIS from home is via SIMS Learning Gateway (SLG) which uses an encrypted VPN back to the data files on the SIMS server at School.

Wireless access is controlled by WPA Encryption, for staff and 6th Formers.

**Staff Own devices (BYOD – Bring Your Own Devices)**

When staff use their own devices, both portable devices such as laptops, mobiles telephones and tablets and home desktop computers, any files containing student or staff personal data must be encrypted at all times. Before any personal data is stored on a home computer, the permission of the DPO should be sort giving the reasons for the request.

Staff will need to sign to say that they are aware of this requirement and this will be renewed annually.

**Anti Virus software**

Sophos updated hourly over the Internet.

**Updates**

All Microsoft Windows updates are installed immediately on servers and client machines via County servers. Client machines run Windows 7.

**CCTV**

We use CCTV to make sure the school site is safe. CCTV is not used in private areas such as toilets. Recordings are stored for the minimum amount of time necessary.

**Keeping data up to date**

Sims Parent Lite App allows Waseley to collect the most up-to-date data about students and parents. Parents can directly update student and parent data.

**Data Protection Impact Assessment**

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The ICO has promoted the use of DPIAs as an integral part of taking a ‘privacy by design’ approach.

The GDPR and the ICO’s website clarify when a DPIA is required. Waseley Hills High School will ensure that whenever any new processes are proposed a DPIA is completed as a matter of course.

**Personal Data Breaches**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This must be done within 72 hours of becoming aware of the breach, where feasible. There should be robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Personal data breaches can include:

* access by an unauthorised third party;
* deliberate or accidental action (or inaction) by a controller or processor;
* sending personal data to an incorrect recipient;
* computing devices containing personal data being lost or stolen;
* alteration of personal data without permission; and
* loss of availability of personal data.

The member of staff discovering the breach should inform their Head of Department and DPO using the Breach advice form.

The DPO may appoint another member of staff to act as Lead Investigating Officer (LIO) or carry out the investigation them-selves. Article 87 of the GDPR makes clear that when a security incident takes place, it should be quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

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.

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people’s rights and freedoms needs to be established. It also needs to be established if the affected person(s) will suffer any harm or loss. If it is likely that there will be any harm suffered then the ICO must be notified.

If no harm will be suffered then a report will not be required, however, if the breach is not reported, it still needs to be documented with justification as to why it was not reported. If in doubt, the school will take advice from the ICO’s Office and err on the side of caution and report rather than not.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the school must also inform those individuals without undue delay.

Any recommendations for further training or a change in procedure shall be reviewed by the School and a decision made about implementation of those recommendations.

**What information must a breach notification to the supervisory authority contain?**

When reporting a breach, the GDPR says you must provide:

* a description of the nature of the personal data breach including, where possible:
* the categories and approximate number of individuals concerned;
* the categories and approximate number of personal data records concerned;
* the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
* a description of the likely consequences of the personal data breach;
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

**Retention**

Article 5 of The GDPR requires that data shall be: “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;”

Waseley Hills High School has a Data Retention Policy which is based on the Information and Records Management Society Retention Guidelines. See below for the link.

<http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf>

**Data Disposal:**

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

<https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf>

The school has identified a qualified source for disposal of IT assets and collections.

The school also uses Shred-it to dispose of sensitive data that is no longer required.

* Third party data processors must be GDPR compliant, it will be a criminal offence to work with suppliers that do not comply

**Rights of access to information (Subject Access Requests):**

There are two distinct rights of access to information held by schools about pupils.

1. Under the General Data Protection Regulations 2016 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the General Data Protection Regulations 2016.

**Subject access request (SAR) procedures**

All individuals whose data is held by us, has a legal right to request access to such

data or information about what is held. A template to make a SAR is available on the school website. We shall respond to such requests within one month and they should be made in writing to:

The Data Protection Officer

Mr N Baker

Waseley Hills High School

New Road

Rubery

B45 9EL

* No charge will be applied to process the request. However additional requests or for duplicate reports to be issued will be charge at a fee to cover the administrative work entailed in completing the request, minimum £10.
* The identity of the person making the SAR will need to be confirmed.

1. Requests for information must be made in writing; which includes email, and be addressed to [Nbaker@waseleyhills.worcs.sch.uk](mailto:Nbaker@waseleyhills.worcs.sch.uk) (Data Protection Officer)**.** If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks will also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

* passport
* driving licence
* utility bills with the current address
* Birth / Marriage certificate
* P45/P60
* Credit Card or Mortgage statement

*This list is not exhaustive*.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. However, children under the age of 13 cannot make a SAR in their own right; it needs to be requested on their behalf. The Data Protection Officer should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The response time for subject access requests, once officially received, is 1 month **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 1 month will not commence until after the request has been received in writing and where necessary identification confirmed.

6. The General Data Protection Regulations 2016 allow exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 1 month statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

**The Rights of the Data Subject**

|  |  |
| --- | --- |
| **Key rights and obligations** | **Overview of requirements** |
| Make information available to individuals | The controller is required to make available to the data subject a range of information, including:   * the identity and contact details of the controller and the data protection officer; * the purpose for which their personal data is being processed; * the existence of their right to exercise any of the below rights; * the legal basis for the processing of their personal data; and * the retention period or criteria used to determine the retention period. |
| Right of access | * Confirmation from the controller whether or not a data subject’s personal data is being processed and, if this personal data is being processed, access to that personal data. |
| Right to rectification | * The controller must, if requested, rectify or complete inaccurate or incomplete personal data. * A controller must notify the competent authority (if any) from which the inaccurate personal data originated, where this personal data has been rectified. * A controller must notify the recipients of personal data, where personal data which been rectified, which has been disclosed by the controller. Similarly the recipient must rectify the processing of the personal data in so far as they retain responsibility for it. |
| Right to erasure or restriction of processing | * The controller is obliged, if conditions are met, to erase personal data or restrict its processing without delay. * A controller must notify the recipients of personal data, where personal data which been erased or restricted which has been disclosed by the controller. Similarly the recipient must erase or restrict the processing of the personal data in so far as they retain responsibility for it. |
| Right not to be subject to automated decision making | * A controller cannot take a significant decision based solely on automated processing unless that decision is authorised by law. |
| Exercise of rights through the Commissioner | * An individual has the option to exercise their rights through the Information Commissioner. |
|  |  |

**What is the period in which a request under these rights must be complied with?**

The controller must provide the requested information or take the appropriate action without undue delay and at least within the “applicable time period”. The applicable time period is within one month of the day on which (unless otherwise specified in separate regulations, and then only up to three months):

• the request was received;

• the controller receives enough information to be able to confirm the identity of the individual;

**Contacts**

If you have any enquires in relation to this policy, please contact the Data Protection Officer, [Nbaker@waseleyhills.worcs.sch.uk](mailto:Nbaker@waseleyhills.worcs.sch.uk)who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner’s Office, www.ico.gov.uk or telephone 0303 123 1113.