

Waseley Hills High School

DATA PROTECTION POLICY

Responsibility: Assistant Headteacher

Author: Mr A W Roll

Date of Issue: December 2015

Review Date: December 2017

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 December
2017



Waseley Hills
High School

DATA PROTECTION POLICY

INTRODUCTION

The Governing Body has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Principal and Governors intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data need to be aware of their duties and responsibilities within these guidelines.

ENQUIRIES

Information about the schools Data Protection Policy is available from the Clerk to the Governing Body. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

Fair Obtaining and Processing

The school undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

“processing” means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

“data subject” means an individual who is the subject of personal data or the person to whom the information relates.

“personal data” means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

“parent” has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

REGISTERED PURPOSES

The Data Protection Registration entries for the school are available for inspection, by appointment, at the school's office. Explanation of any codes and categories entered is available from the Head of ICT, who is the person nominated to deal with Data Protection issues in the school. Registered purposes covering the data held at the school are listed on the Registration and Data Collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

DATA INTEGRITY

The school undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Head of ICT to ensure that obsolete data are properly erased.

SUBJECT ACCESS

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves

it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the school's policy is that:

Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.

Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

PROCESSING SUBJECT ACCESS REQUESTS

Requests for access must be made in writing.

Students, parents or staff may ask for a Data Subject Access form, available from the school office. Completed forms should be submitted to the Clerk to the Governing Body. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 School days in accordance with the current Education (Pupil Information) Regulations.

AUTHORISED DISCLOSURES

The school will, in general, only disclose data about individuals with their consent. However there are circumstances under which the school's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

Student data disclosed related to education and administration necessary for the school to perform its statutory duties and obligations.

Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.

Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.

Only authorised and trained staff are allowed to make external disclosures of personal data.

Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work.

The school will not disclose anything on student s' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An "illegal disclosure" is the release of information to someone who does

not need it, or has no right to it, or one which falls outside the school's registered purposes.

Data and Computer Security

The school undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the School should in the first instance be referred to the Clerk to the Governors.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from:

Information and Commissioner's Office (ICO): www.ico.gov.uk

The Guide to Data Protection provided by the ICO Data Protection Act 1998.

DATA PROTECTION POLICY

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname.....Fore Names.....
Address
.....
.....Postcode
Telephone Number

Are you the person who is the subject of the records you are enquiring about YES/NO (i.e. the "Data Subject")?

If NO –

Do you have parental responsibility for a child who is the "Data Subject" of the YES/NO records you are enquiring about?

If YES,

Name of child or children about whose personal data records you are enquiring
.....
.....
.....
.....

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information.

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

Name of "Data Subject" (or Subject's Parent)

Dated:

Data Protection Policy and Code of Practice for Information

Sharing and Exchange with other Public Agencies

This policy will be continually reviewed to ensure that improvements are made and that good practice is maintained consistent with legislation (Data Protection Act 1998) and compliance advice.

Relevant Legislation:

The Education (Pupil Information)(England) Regulations 2000;
The Data Protection Act 1998;
Data Protection (Subject Access Modification)(Education) Order 2000.
The Children's Act 1989.

The School is registered under the Data Protection Act 1998, and the Notification shall be renewed as required. Details of the Notification to the Register may be obtained from the School, and are implicit within the Policy and Guidelines contained within this policy document. The School complies fully with the Data Protection principles, which state that personal information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than is necessary
- Processed in accordance with an individual's rights
- Kept secure
- Not transferred without adequate protection

Such principles shall be reflected in records and information kept with respect to both electronic and manual systems.

Staff and students shall be made aware of:

The nature of the information collected about them;
The purpose(s) for which personal information will be held;
What such information will be used for;
Who, other than internally, may the data / information be disclosed to.

Unless the information is subject to other enabling legislation, or the possibility of the sharing such information has been made explicit, informed consent must be obtained before such information is passed to another organisation or individual.

The Collection of Student Data and Information

The nature and sources of information:

The transfer of a student's educational record when a student changes School (either at age 11, or within Key Stages 3 and 4). The School will fully comply with guidance contained in DfES Circular 17/89: *The Education (School Records) Regulations 1989*;

and, DfES Circular 17/99: *Reports on pupil Achievement*. The Common Transfer Form will be utilised.

At transfer between Year 6 from within the LEA information is collected, largely through discussion with relevant staff, on such issues as medical knowledge; Special Educational Needs; learning aptitude and characteristics; and behavioural characteristics. This information is noted and forms part of the information contained in the student's record.

The completion of the School *Entry Form* provides such information as name, address, contact data, emergency contact information, medical, ethnicity and religious information. This information is kept within the School's student database.

The results of screening tests, baseline data testing and diagnostic tests are kept, together with regular assessment and achievement results.

Statutory information such as attendance, punctuality, Key Stage assessment data (including post 14 achievement data – GCSE; CoE; GNVQ; NVQ).

Behavioural data and information (*see Behavioural Management Policy*) relating to rewards and sanctions deployed by the School (including Exclusion data).

Any relevant data and information that allows the School to discharge its statutory responsibilities, including the care and welfare of students. Such information may include changed family circumstances (for example divorce, bereavement, financial hardship) and Child Protection documentation, and may be obtained from a number of sources including teaching and support staff, Learning Mentors, and other agencies.

The keeping of Data and information

Data and information on students is kept in four different locations:

Centrally held electronic information:

The School records data and information on students within the SIMS student database on the Administrative ICT Network.

Such information includes that relating to:

- name;
- gender;
- date of birth;
- Unique Pupil Number;
- address;
- contact information;
- legal guardianship;
- medical information;
- emergency contact information;
- ethnicity;
- religion;
- doctor;
- method of travel to School;
- attendance;
- punctuality;
- achievement;
- photograph.

Centrally held manual records

The student's form tutor and Head of House are responsible for the upkeep of the student's record which, in addition to much of the information listed above, also includes documentation relating to the individual student arising from their time in School. Such information includes:

Pupil Information Notes

copies of letters sent to parents;
copies of Individual Education Plans
copies of Pastoral Support Plans
medical details and guidance;
copies of reports
copies of Certificates and Achievement Awards made
subject option information (KS4);
information collected for specific purposes, such as referrals to

Learning

Support or the Inclusive Learning Base

student target sheets completed
letters from parents and others acting for the student
Copies of letters sent home from the School;
Special Educational Needs documentation including reviews;
contact with other agencies such as Young Offenders Team.

Electronic and manual records held by the Learning Support department

The Learning Support Department, under the direction of the SENCO, maintain records that relate specifically to students with Special Educational Needs. Such information is maintained either electronically, or in manual form and includes such information as:

Statements of Special Educational Needs;
Individual Education Plans
Pastoral Support Plans
medical details and guidance;
information collected for specific purposes, such as referrals to

Learning

Support or the Student Service Base

Student Service Base reintegration plans;
letters from parents and others acting for the student
review documentation
screening and diagnostic test data;
achievement data relating to programmes undertaken;
copies of relevant letters from parents and others acting for the student
target information and Learning Support Assistant logs;
record of contacts made with respect to an individual student

4. Individual Teacher and Learning Support Assistant records:

Individual teachers and Learning Support assistants are required to maintain records in order that they may adequately teach and support students relevant to their ability and circumstances. It is expected that they shall maintain records that detail:

- Attendance at lessons;
- Baseline and diagnostic data, including where relevant IEP's;
- Achievement data relevant to their teaching and learning activities;
- target data;
- Behavioural information, including such things as individual study
- Completion, and behavioural support plans.

The Sharing of Data and Information

The Data Protection Act came into force on 1st March 2000. It regulates the holding and processing of personal data, that is, information and data relating to students within School.

To ensure compliance with the Data Protection Act non-sensitive personal data shall be processed fairly and lawfully, and shall not be processed unless at least one of the following conditions is met:

- The individual whose records are kept by the School must provide consent;
- The School must have a legal requirement or basis to hold information about them;
- Have a need to hold it for the performance of a contract, or for the taking of steps with a view entering into a contract;
- Have a reason to hold it in the legitimate interests of the organisation, unless the processing may prejudice the rights and freedoms or legitimate interests of the individual;
- To protect the individual's vital interests;
- For the administration of justice;
- Information is processed in circumstances specified by order of Government.

For sensitive information personal data shall be processed fairly and lawfully only if at least one of the following conditions is also met (in addition to those listed above):

- The individual has provided their explicit consent;
- The information is required to be held in compliance with employment law;
- To protect the individual's vital interests in cases where consent cannot be given, or to protect the interests of another person where consent has been unreasonably withheld;
- The processing is carried out by a not-for-profit organisation or a body that exists for political, philosophical, religious or trade union purposes;
- The information has been made public as a result of steps deliberately taken by the individual;
- The processing is necessary with respect to legal proceedings, for obtaining legal advice, or for establishing, exercising or defending legal rights;
- For the administration of justice;
- Have a legal requirement or basis to hold information (for example, to carry out statutory functions);
- The processing is necessary for medical purposes;
- Information that consists of racial or ethnic origin can be held to ensure and monitor equality of opportunity or treatment;
- Information is processed in circumstances specified by Government.

Sensitive information, as defined by the Data Protection Act, is information that relates to:

- Racial or ethnic origin;
- Physical or mental health condition;
- Sexual life;
- Religious or other beliefs;
- Commission or alleged commission of offences;
- Any proceedings for any offence committed (or alleged, the disposal of such proceedings or the sentence of any court in such proceedings);
- Political opinions;
- Trade union membership.

Within the School:

Between those employed by the School, and accountable to the Principal, it is recognised that the fullest sharing of data and information between those responsible for the teaching, welfare and care of the student leads to the most benefit for the student.

(For example, information about the bereavement of a close family member should be shared by all those likely to come into responsible contact with the student in order for appropriate care and support to be established.)

It is however inherent that any and all such information should be kept confidential between members of staff within the School and not shared with others.

It is a matter of professional judgement as to whether information disclosed by a student is of necessity shared by all within the School, if uncertain members of staff should consult with their line manager.

However, any information disclosed relating to physical, sexual or emotional abuse, or neglect of students will be fully subject to the School's Child Protection Policy and Guidelines.

Any and all manual records kept by the School relevant to individual students, no longer required, must be handed in to the School office for shredding.

Student records held centrally, on the student's departure from the School, will be archived and stored for a minimum of ten years. The Office Manager will be responsible for the upkeep of the archive.

Teachers and Classroom Support Assistants / Mentors will maintain records for the students that they taught and supported, whether manual or electronic, for a minimum of five years. They should also be maintained for this period if the member of staff concerned leaves the employment of the School.

At times individual student level information is required for illustrative purposes by processes that the School is subjected to by other legislation, guidance or practice.

Examples include Ofsted Inspection; Threshold Assessment; Performance Appraisal and Target Setting. The School will be explicit to students and parents in this respect,

though individual students should not be named in any publication or report resulting from such processes.

Information with respect to named individual students should not be produced for any audience whereby the information may thereby enter into the public domain, without the express permission of the student involved. School based examples include:

School Newsletters to parents and the community;
Reports to the Governing Body;
Review and evaluation documentation for other than internal use;
Any and all documentation used for training or illustrative purposes to persons outside of the School.

Student teacher's, supply staff and others professionals working on a temporary basis as a member of staff within the School, accountable to the Principal, will be required to adhere to the principles of data and information protection outlined.

With Outside Organisations, Agencies and Individuals:

Unless the information is subject to other enabling legislation, or the possibility of the sharing such information has been made explicit, informed consent must be obtained before such information is passed, by the School, to another organisation, agency or individual.

Students and parents will be made explicitly aware that it is practice to share student level information, which may include personal information, with respect to:

Feeder Primary Schools:

Achievement data and the results of benchmark testing.

LEA:

Information and Data required and requested by the Local Education Authority in pursuit of their responsibilities and obligations, including the administration of the SEN Code of Practice. All such data and Information is protected under the Data Protection Act 1998.

QCA / DfE

Assessment, achievement and attendance data at non specific student level.

Post 16 institutions and organisations:

Information and data with respect to achievement, actual and predicted / target data, together with essential core personal data, with post 16 educational institutions or training establishments. This information will normally be contained within their Record of Achievement / Progress File.

School Medical Service:

Any information relating to the student's health, care and welfare both within the School and in his/her life that could affect the quality of life and achievement of the young person.

Social Services:

Any information disclosed relating to physical, sexual or emotional abuse, or neglect of students subject to the Children's Act 1989 using the procedures specified in the School's Child Protection Policy and Guidelines.

Police:

Requests for the disclosure of information for purposes, such as the prevention or detection of crime, prosecution or apprehension of offenders, must be authorised by a senior member of staff (Principal; Vice Principal; Assistant Principal, Head of Year), and only when they have verified that it is a genuine request.

Educational Welfare Service:

Attendance data and information relating to family circumstances pertaining to the student's ability to attend School regularly and to effect.

Careers Advisory Service:

Information and data with respect to achievement, actual and predicted/target data, together with essential core personal data to enable effective careers guidance to take place.

When exchanging or sharing data and information with other institutions, organisations, agencies or individuals the following principles should be observed:

The School is to assume that all students are competent in their own right to make decisions and provide consent for the sharing and exchange of data and information with other institutions, organisations, agencies or individuals. However, parents and or guardians should be made aware of the exchange or sharing of data and information with other institutions, organisations, agencies or individuals both through the School Prospectus and by clear statements on data capture forms.

When sharing and exchanging data and information with other institutions, organisations, agencies or individuals the minimum amount of data or information should be provided, exchanged or shared, its purpose clearly identified and any further processing of such data or information by that institution, organisation, agency or individual reported to the School.

School staff should be aware that verbal exchange of data or information can be misunderstood, misinterpreted, or misrepresented, and it should be avoided.

The institutions, organisations, agencies or individuals receiving information from the School will undertake not to disclose, share or exchange such information with other institutions, organisations, agencies or individuals without first obtaining further informed consent from the student unless the original consent covered such eventualities.

Information and data shared or exchanged with other institutions, organisations, agencies or individuals should be first checked for accuracy and reliability by the School. Any information not based upon established fact should be clearly identified as opinion or hearsay.

It is the responsibility of the receiving institution, organisation, agency or individual to inform the School of any and all information and data that is discovered to be out of date, inaccurate or unreliable.

Institutions, organisations, agencies or individuals that have disclosed to them data or information relevant to the care and welfare, or the effective teaching and management of Waseley Hills students, should take the necessary steps to achieve the consent of the young person to share such information with the School, which they should then undertake.

Institutions, organisations, agencies or individuals receiving information or data from the School must take all reasonable precautions to protect such personal information or data from unauthorised or unlawful processing or use, and against its accidental loss, destruction or damage.

Institutions, organisations, agencies or individuals unable to agree to these principles will not be made party to personal information concerning Westfield School students except where this is covered by enabling legislation or associated Orders.

Access to Data and Information held by the School

Every student, ex-student, employee, ex-employee or where appropriate a person legally acting on their behalf, has the right to access the personal data and information which relates to them, either computerised or paper records.

Requests to see, or receive copies of School records, should be made in writing to the Principal. A charge may be made to cover the cost of researching and copying the records, according to the number of pages. Requests may be returned for data to verify the identity, or to provide information necessary to locate the data and information held about them (for example, in the case of former students / employees the dates between which he / she attended the School).

Examples of fees that may be charged:

1 to 19 pages £3
50 to 59 pages £10
100 to 149 pages £15
200 to 249 pages £25

Other fees that may be charged;

Postage
Governor's time
Legal fees

Some information may be withheld from the student. For instance, if it may cause harm to the physical or mental health of the student or a third party; information, which may identify third parties (for example, other students), and information that forms part of court reports. Information may also be withheld if in that particular case it would hinder the prevention or detection of crime or the prosecution or apprehension of offenders to provide it.

In addition, students / employees are also entitled to be given a description of the personal data and information which makes up the School record, together with details of the purposes for which the data is processed, the sources of the data and

information, and the institutions, organisations, agencies or individuals to which the data and or information may be disclosed to.

Parents also have their own independent right of access to the official educational records of their children. In essence the information to which parents are entitled and the exemptions are the same as for students. A parent seeking access to an educational record does not however have a right of redress under the Data Protection Act unless he / she is acting on behalf of their child. As parents have an independent right to access student records the students themselves have no right to prevent it.

If a request for information under the Act is ignored the matter may be referred to the Information Commissioner, or an application for disclosure can be made to the courts. Parents requesting the information, unless acting on behalf of their child, in the first instance should contact the governing body, after that the DfES, or, as a last resort, the courts.

Further information about the Data Protection Act (1998) can be obtained from the Commissioner's web site (www.dataprotection.gov.uk), requested from an information line (01625 545745), or by post from:

The Office of the Information Commissioner,
Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Students, or where appropriate a person legally acting on their behalf, may make a complaint about the way in which information about them is held, processed or disclosed by writing to the Principal, after that the Governing Body, the DfES, or as a last resort, the courts.