IDSALL
DATA PROTECTION POLICY
2018-19

Sponsorship & Review

1	**Sponsor**

Mr D. Crichton, Deputy Headteacher

2	**Reviewed**

May 2018

3	**Revision Date**

May 2019

POLICY DOCUMENT	**Data Protection Policy 2018**
STATUTORY FOR ACADEMY SCHOOLS	**Statutory**
Legislation: Education/Other	Statutory document for Academy Schools
Lead Member of Staff	D. Crichton – Deputy Headteacher
Lead Governors (monitoring)	D. Brammer
Publication /Revision Date	October 2015 / May 2018
Governor Committee	Behaviour and Safety Committee
Committee Approval Date	10th May 2018
Full Governors Ratification Date	
Review Frequency	1 year
Date of next review	May 2019
Publication date: **School Website** **Staff Information folder**	May 2018
Chair of Governing Body signature	
Purpose	To ensure that the Headteacher and the Governing Body act in accordance with the law on Data Protection
Supporting documents	eSafety policy Freedom of Information Act –policy

The school's data protection policy sets out, in writing, the manner in which personal data on staff, students and other individuals (e.g. parents, members of the governing body and other stakeholders) are kept and how the data concerned is protected.

We shall apply the principles of the Data Protection Act 1998 to all data processed:

1. Processed fairly and lawfully.
2. Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes.
3. Accurate and, where necessary, kept up to date.
4. Adequate, relevant and not excessive in relation to the purposes for which it is processed.
5. Not kept for longer than is necessary for those purposes.
6. Processed in accordance with the rights of data subjects under the DPA.
7. Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.
8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

The Deputy Head with responsibility for Data Protection initially drafted the policy. The Senior Leadership Team then reviewed it before the policy was then shared with staff, reviewed and updated before being ratified by the governing body.

To what does the policy apply?

The policy applies to the keeping and processing of personal **data**, both in manual form and on computer, including **personal data** held on school staff, students and parents.

Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: ***Racial or ethnic origin*** ***Political opinions*** ***Religious beliefs, or beliefs of a similar nature*** ***Where a person is a member of a trade union*** ***Physical and mental health*** ***Sexual orientation*** ***Whether a person has committed, or is alleged to have committed, an offence*** ***Criminal convictions***
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

The Data Controller

Idsall school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Headteacher acting for the governing body in exercising the functions involved.

Idsall school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

The Data Protection Officer

The role of the data protection officer will be fulfilled by a team consisting of the Deputy Head with responsibility for Data Protection, the Finance Manager and the Network Manager. The governors believe that this will mitigate any issues with conflicts of interest and will provide adequate "checks and balances" as well as the combined expertise to fulfil the role effectively in the context of our organisation. Mr. D Crichton, Deputy Head will be the named Data Protection Officer for the school and this will be the contact given to the ICO.

Role and Responsibilities

The governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the headteacher, or the deputy head in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

Legislation and Guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force in May 2018.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

This policy complies with our funding agreement and articles of association.

What this policy intends to achieve.

1. To ensure that the school complies with the Data Protection Acts.

2. To ensure compliance by the school with the eight principles of data protection as set down by the Data Protection Commissioner based on the Acts.

3. To ensure that the data protection rights of students, staff and other members of the school community are safeguarded.

The GDPR provides the following rights for individuals:

a) The right to be informed
b) The right of access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling.

Content of the Policy

The policy content has been divided into two sections as follows:

A. Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case.

B. Details of the arrangements in place to ensure compliance with the eight principles of data protection.

A. Details of all personal data which will be held and the purpose(s) for collecting the data in each case

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, addresses, employee or teacher number, national insurance number, etc)
- special categories of data including characteristics information (such as gender, age, ethnic group, etc)
- contract information (such as start dates, hours worked, post, roles, salary and payroll information, etc)
- work absence information (such as number of absences and reasons including relevant medical information, etc)
- qualifications (and, where relevant, subjects taught)
- employment history and references

Why we collect and use this information to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- fulfil our "Caring about Sickness" (CAS) obligations
- inform the development of recruitment and retention policies
- enable individuals to be paid
- support Safer Recruitment

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- exclusions / behavioural information
- Assessment information (such as KS2, KS3, KS4, post-16)
- relevant medical information
- special educational needs information

We use the pupil data to:

- support pupil learning
- monitor and report on pupil progress
- provide appropriate pastoral care
- meet our safeguarding obligations
- assess the quality of our services
- comply with the law regarding data sharing

The categories of Governor information that we collect, hold and share include:

- Name, address and contact details of each member of the governing body
- Records in relation to appointments to the board
- Minutes of governing body meetings and correspondence to the board which may include references to particular individuals.

We use the governor data to:

- keep a record of board appointments,
- document decisions made by the board.
- communicate with members of the Governing Body

B. Details of arrangements in place to ensure compliance with the eight principles of data protection

Context

The policy sets down the arrangements in place to ensure that all personal data records held by the school are obtained, processed, used and retained in accordance with the following eight principles of data protection (based on the Data Protection Acts):

1. Processed fairly and lawfully.
2. Obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes.
3. Accurate and, where necessary, kept up to date.
4. Adequate, relevant and not excessive in relation to the purposes for which it is processed.
5. Not kept for longer than is necessary for those purposes.
6. Processed in accordance with the rights of data subjects under the DPA.
7. Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.
8. Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

- *One of the most important changes under the GDPR is to the rights of children. The GDPR identifies children as "vulnerable individuals" who need "special protection".*
- ***If you are relying on consent** as your lawful basis for processing personal data, then **for children under 16** you will need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.*
- *You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. **Sometimes using an alternative basis is more appropriate and provides better protection for the child**.*

1. Obtain and process information fairly and lawfully:

- In order to ensure that staff members, parents/guardians and students are made fully aware when they provide personal information of
    - the identity of the persons who are collecting it,
    - the purpose in collecting the data,
    - the persons or categories of persons to whom the data may be disclosed
    - any other information which is necessary so that processing may be fair:

a) When requesting personal information, the statement in Appendix A will be included on relevant forms. (LD – Admin Team Leader)

b) ***All staff members will receive annually, a copy of the Privacy Notice for School Workforce (Appendix E) in their staff pack on the first school day in September.*** (MJ – Headteacher's PA)

c) All parents and pupils will have access to the Privacy Notice for Pupils (Appendix D) via the school website. (www.idsallschool.org) (HM – IT Technician). ***A copy will also be added to the Information Pack given to all new starters when they join Idsall School.*** (VH – Business Manager)

- In order to ensure that personal information is processed fairly in accordance with the Data Protection Acts:

    d) Consent will be obtained from staff members, parents/guardians or students, where required (see above). (VH – Business Manager)

    e) However, if it is deemed that consent is not required, then the processing must be identified as being necessary for one of the following 'lawful' reasons – (DC – Data Protection Lead)

1. A contract with the individual:
- the performance of a contract to which the data subject is party
- in order to take steps at the request of the data subject prior to entering into a contract

2. Compliance with a legal obligation:
- compliance with a legal obligation, other than that imposed by contract

3. Vital interests:
- to prevent injury or other damage to the health of a data subject
- to prevent serious loss or damage to property of the data subject
- to protect the vital interests of the data subject where the seeking of
- the consent of the data subject is likely to result in those interests being damaged

4. A public task:
- for the administration of justice
- for the performance of a function conferred on a person by or under an enactment
- for the performance of a function of the Government or a Minister of the Government
- for the performance of any other function of a public nature performed in the public interest by a person

5. Legitimate interests:
- for the purpose of the legitimate interests pursued by a data controller
- except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

(see Appendix B for further details)

Special category data

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- ethnicity
- nationality / race
- proficiency in English
- first language
- SEN info
- LAC info
- disability
- biometrics
- health

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

- In order to ensure that sensitive personal information will be processed fairly in accordance with the Data Protection Acts:

    f) ***Explicit consent will be obtained from staff members, parents/guardians or students, where required.*** (LG – Admin Team Lead)
    i.e. the data subject has been clearly informed of the purpose/s in processing the data and has supplied his/her data with that understanding

    g) However, if it is deemed that explicit consent is not required, then the processing must be identified as being necessary for one of the 'lawful' reasons above. (DC - Data Protection Lead)

    h) We will <u>also</u> identify whichever of the following special category conditions is the most appropriate in the circumstances. (DC - Data Protection Lead)
    The difference is that you will <u>also</u> need to satisfy a specific condition under Article 9.

NOTE: The choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9.

1. for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment

2. to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where, consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent

3. to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld

4. it is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation

5. the information being processed has been made public as a result of steps deliberately taken by the data subject

6. for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights

7. for medical purposes

8. is carried out by political parties or candidates for election in the context of an election

9. for the purpose of the assessment or payment of a tax liability

10. in relation to the administration of a Social Welfare scheme.

(see Appendix C for further details)

NOTE: We collect and use pupil information under the submission of the school census returns, including a set of named pupil records. This is a statutory requirement on schools under Section 537A of the Education Act 1996.

Putting the school census on a statutory basis:

- **means that schools do not need to obtain parental or pupil consent to the provision of information**
- **ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils**
- **includes a basis from Article 6, and one from Article 9 where data processed is special category data from the GDPR-from 25 May 2018**

2. Keep it only for one or more specified, explicit and lawful purposes

- In order to ensure that the persons whose data is collected know the reason/s why it is collected and kept:

    a) When requesting personal information, the statement in Appendix 1 will be included on relevant forms. (LD – Admin Team Lead)

    b) All staff members will receive annually, a copy of the Privacy Notice for School Workforce (Appendix E) in their staff pack on the first school day in September. (MJ – Headteacher's PA)

    c) All parents and pupils will have access to the Privacy Notice for Pupils (Appendix D) via the school website. (www.idsallschool.org) (HM – IT Technician). ***A copy will also be added to the Information Pack given to all new starters when they join Idsall School.*** (VH – Business Manager)

- In order to ensure that school management are aware of the different sets of data which are kept and the specific purpose of each:

    d) A central record will be kept in the Policies/GDPR folder on the school network. (DC – Data Protection Lead). ***This record will contain information on:***

    - Type of data held
    - What personal data is stored
    - Is data identified as "special category data"
    - How it was collected
    - Was consent obtained?
    - Other lawful reason it is collected and processed
    - For "special category data" - specific condition under Article 9
    - Where the data is stored
    - Is it held/shared with a 3rd party? If YES, who…
    - Is a GDPR-compliant contract in place with the third party?
    - Security measures that are in place
    - Who has access to it?
    - Is the data ever taken off-site?
    - Where and why is it shared externally, if at all?
    - How do we ensure it is accurate and up to date?
    - Retention period
    - Method of disposal at end of retention period.

- In order to ensure that the purpose for which the data is collected and kept is a lawful one:

    e) The central record, kept in the Policies/GDPR folder on the school network, identifies the lawful reason and will be reviewed at the same frequency as the review of this policy. (DC – Data Protection Lead).

In order to ensure that data is used only in ways consistent with the purpose/s for which it was obtained and to ensure that data is disclosed only in ways consistent with that purpose:

f) ***The school's Senior Information Risk Officer (SIRO) is*** Mr Crichton (Deputy Head)***. This person will keep up to date with current legislation and guidance and will:***

- *determine and take responsibility for the school's information risk policy and risk assessment*
- *appoint the Information Asset Owners (IAOs**)***

g) ***The IAOs will manage and address risks to the information and will understand :***

- *what information is held, for how long and for what purpose,*
- *that data can only be used in ways consistent with the purpose/s for which it was obtained and that data is disclosed only in ways consistent with that purpose*
- *how information has been amended or added to over time,*
- *who has access to protected data and why.*

Information Asset Owners (IAOs)		
Type of data	***Role at Idsall School***	***Postholder***
Student, parents and staff records (inc First Aid)	*Admin Team Lead*	*L. Donegani*
SIMS data and pupil records	*Admin Team Lead*	*L. Donegani*
SEN data, records and documentation	*SENCO*	*C. Cork*
Centrally held Assessment and tracking information	*Data Manager*	*D. Langton*
Exam data including entries, grades and marks	*Exams Officer*	*A-M. Evans*
Pupil Library information	*Librarian*	*P. Hazlehurst*
Finance and personnel / payroll information	*Business Manager*	*V. Hulme*
Child protection files and information	*SENCO/CPO*	*C. Cork/J. Reeve*
Extended services (CHAT, student support)	*Asst. Head/Deputy Head*	*C. Cork/R. Thorley*
Behaviour reports and logs	*KS3/KS4 Managers*	*H. Lynne/P. Lamb*
Admissions, exclusions, CAS, EVC, recruitment etc	*Headteacher's PA*	*M. Johnston*
ICT and Network Management	*Network Manager*	*A. Groucutt*
CCTV	*Site Manager*	*R. Hughes*

h) Everyone ***in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.***

i) Governors ***are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.***

3. Keep data accurate, complete and up-to-date:

Note: *While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.*

Right to Rectification

a) To comply with these provisions Idsall School will take reasonable steps to ensure the accuracy of any personal data we obtain; specifically

i. parents will be given a copy of the data collection sheet every two years (when their child is in Y8 and Y10) in order to check the accuracy of personal data held. (LD – Admin Team Lead)

ii. parents are also reminded that it is their responsibility to inform the school should any information change in the meantime. (LD – Admin Team Lead)

iii. ***employees will be given the equivalent data collection sheet annually for them to check their personal data.*** (VH – Business Manager)

iv. ***ensure that the source of any personal data is clear and recorded in the central record to be kept in the Policies/GDPR folder on the school network.*** (DC – Data Protection Lead)

b) Where there is a challenge to the accuracy of the data held, Idsall School (VH – Business Manager) ***will:***

i. ***carefully consider any challenges to the accuracy of information***

ii. seek documentary evidence from the data subject to support the challenge

iii. consider whether it is necessary to update the information.

c) Where the challenge is upheld, Idsall School will amend the personal data of the data subject, as requested, and inform the data subject in writing that the changes have been made. (LD – Admin Team Lead)

4. Ensure that data is adequate, relevant and not excessive:

Note: *While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.*

a) In order to ensure the information held, is adequate in relation to the purpose/s for which it is kept, the central record, kept in the Policies/GDPR folder on the school network, will be reviewed with the same frequency as this policy. (DC – Data Protection Lead)
This record will contain information on:

- Type of data held
- What personal data is stored
- Is data identified as "special category data"
- How it was collected
- Was consent obtained?
- Other lawful reason it is collected and processed
- For "special category data" - specific condition under Article 9
- Where the data is stored
- Is it held/shared with a 3rd party? If YES, who…
- Is a GDPR-compliant contract in place with the third party?
- Security measures that are in place
- Who has access to it?
- Is the data ever taken off-site?
- Where and why is it shared externally, if at all?
- How do we ensure it is accurate and up to date?
- Retention period
- Method of disposal at end of retention period.

5. Retain data for no longer than is necessary:

Note: *While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.*

In general, personal data should not be kept for any longer than is necessary to fulfil the function for which it was first recorded.

a) ***We will follow the retention period guidelines outlined in the Idsall School Retention Guidelines Policy.*** (VH – Business Manager)

b) ***Retention times cannot be rigidly prescribed to cover every possible situation and Idsall School will exercise its judgement in this regard in relation to each category of records held.*** (VH – Business Manager)

Note: *The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge post dates their 18th birthday. While schools may wish to draw up their own policies as to how long to retain such records, it would appear prudent not to destroy records likely to be relevant in litigation at least until the* ***six year limitation period*** *has expired.*

5.1 Disposal of records

At the end of the agreed retention period *(see retention period guidelines outlined in the Shropshire Council Retention Guidelines for Schools)*, personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

a) ***Paper-based records will be shredded or incinerated, and electronic files overridden.***

b) ***An outside company may be used to shred paper-based records.***

c) ***Any paper-based records that contain personal data must not be placed in waste paper bins or recycling boxes, but must be placed in a 'shredding bag'.*** (ALL Staff)

   i. ***Whilst being filled (over a period of time) 'shredding bags' must be stored in a locked staffroom or office.*** (ALL Staff)

   ii. ***The 'front office' will notify staff when to deliver 'shredding bags' to the front of school ready for collection by the outside company.*** (LD – Admin Team Lead)

d) ***An outside company may be used to safely dispose of electronic records.*** (AG – Network Manager)

6. Rights of Data Subjects

The rights of individuals are:

- a right of access to a copy of the information comprised in their personal data;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to prevent processing for direct marketing;
- a right to object to decisions being taken by automated means;
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- a right to claim compensation for damages caused by a breach of the Act.

6.1 Subject access requests

Under the Data Protection Act 1998, individual data subjects have a right to request access to information that Idsall School holds about them. This is known as a subject access request.

a) On receiving a subject access request from any individual (subject to the restrictions noted below) about whom Idsall School keeps personal data, we shall furnish the data subject with the following information:

- ***a copy of the data which is kept about him/her***
- ***the purpose/s for processing his/her data***
- ***the identity of those to whom the data is disclosed***
- ***the source of the data, unless it is contrary to public interest***
- ***the logic involved in automated decisions***
- ***a copy of any data held in the form of opinions, except where such opinions were given in confidence.***

b) Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- ***The pupil's name***
- ***A correspondence address***
- ***A contact number and email address***
- ***Details about the information requested***

c) All subject access requests should be addressed to Mrs. V. Hulme, Business Manager***. If the initial request does not clearly identify the information required, then further enquiries will be made.***

d) The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. (VH - Business Manager)

- ***Evidence of identity can be established by requesting production of a valid:***
  - ***passport***
  - ***driving license***
  - ***utility bills with the current address***
  - ***Birth / Marriage certificate***
  - ***P45/P60***
  - ***Credit Card or Mortgage statement***
  - *NOTE: This list is not exhaustive.*

e) In the case where there have been any legal proceedings which may limit the right of one or both parents to access information about their child, Idsall School will ensure we have a clear understanding of any ruling. (VH - Business Manager)

- Note: If spouses are separated and one of them has obtained an order for custody but both of them remain guardians, then both of them are entitled to be involved in important decisions which affect the child.

f) VH - Business Manager ***will co-ordinated procedures to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made?***

g) VH - Business Manager ***will co-ordinated procedures to rectify or erase any inaccurate information as identified by the individual on whom the data is kept.***

h) Subject access requests for all or part of the pupil's educational record will be provided within 20 school days. (Weekends do not count as school days.)

NOTE: if a request is made prior to any official school holiday, we will only count school days as days when staff and pupils are required to attend. We will write to the requestor to confirm these timings should a holiday occur within the 20 day period. (NOTE: The ICO specifies that a Subject Access Request should be fulfilled within one calendar month.)

i) We will provide a copy of the information free of charge. However, the headteacher may make a charge for the provision of information, dependent upon the following: (VH - Business Manager)

- ***when a request is manifestly unfounded or excessive, particularly if it is repetitive.***
- ***when requests are made for further copies of the same information.***

j) Any fee charged will be based on the administrative cost of providing the information. The table in Appendix F, below summarises the charges that will apply.

k) Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Headteacher ***can:***

- ***charge a reasonable fee taking into account the administrative costs of providing the information (see Appendix F); or***
- ***refuse to respond.***

If the Headteacher ***refuses to respond to a request, he will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.***

l) The school <u>will not reveal</u> the following information in response to subject access requests: (VH - Business Manager)

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Access requests by students

m) Subject to the information below, students aged 16 and over are entitled to access their personal information in accordance with the Data Protection Acts. Requests must be submitted as described above. (VH - Business Manager)

- Students under 16 years of age can be given access to their personal information, depending on the age of the student and the nature of the record i.e. it is suggested that:
    - if the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
    - if the record is of a sensitive nature, it would be prudent to seek parental/guardian consent
    - if a student has some disability or medical condition that would impair his or her ability to understand the information, or if disclosure would be likely to be harmful to the individual concerned, parental/guardian consent should be sought.

Parental requests to see the educational record

n) Subject to the information below, parents have the right of access to their child's educational record, free of charge, within 20 school days of a request. Requests must be submitted as described above. (VH - Business Manager)

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.
For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may not be granted without the express permission of the pupil.
If parents ask for copies of information, they will be required to pay the cost of making the copies.

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

Exceptions to note:

- Schools should note that data protection regulations prohibit the supply of:

  - health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate "health professional", normally the patient's own doctor

  - personal data obtained in the course of carrying on social work if that would cause serious harm to the health or emotional condition of the data subject concerned. The regulations apply to social work carried on by Ministers, local authorities, the HSE or any other such bodies receiving financial assistance from public funds.

  - examination marks and personal data contained in examination scripts

  - **Confidential References** - Personal data is exempt from an individual's right of subject access if it comprises a confidential reference that an organisation gives (or is to give) in connection with education, training or employment, appointing office holders, or providing services. The exemption only applies to references you give, and not to references you receive.

  - **NOTE**: further exemption may apply and details can be found on the ICO website : https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/.

o) 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. (LD – Admin Team Lead)

p) 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. (LD – Admin Team Lead)

q) 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. (LD – Admin Team Lead)

r) ***All information will be reviewed prior to disclosure and if there are any concerns over the disclosure of information then additional advice will be sought from the ICO.*** (Data Protection Officer)

s) Complaints about the above procedures should be made to the Chairperson of the Governing Body ***who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioners Office. Contact details of both will be provided with the disclosure information.***

6.2 Right to restrict processing

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.

a) The right to supress processing will be stated in the Privacy Notices available to all data subjects. (Appendix D and Appendix E)

b) If a data subject submits a written request to Mr. D Crichton, Deputy Headteacher ***requesting that we 'block' or supress processing of their personal data, an assessment of the reasons given by the data subject will be made in accordance with the guidance on the ICO website.***

c) If the circumstances of the request meet the guidance on the ICO website, we will inform the data subject in writing that we will retain the information held, but will no longer process it. (Data Protection Officer)

6.3 Right to Object

a) The right to object will be stated in the Privacy Notices available to all data subjects. (Appendix D and Appendix E)

b) If a data subject submits a written request to Mr. D Crichton, Deputy Headteacher ***objecting to the processing of their personal data, an assessment of the reasons given by the data subject will be made in accordance with the guidance on the ICO website.***

c) If the circumstances of the request meet the guidance on the ICO website, we will inform the data subject in writing that we will longer process their personal data. (Data Protection Officer)

6.4 Right to Erasure

a) The right to erasure will be stated in the Privacy Notices available to all data subjects. (Appendix D and Appendix E)

b) If a data subject submits a written request to Mr. D Crichton, Deputy Headteacher ***requesting erasure of their personal data, an assessment of the reasons given by the data subject will be made in accordance with the guidance on the ICO website.***

c) If the circumstances of the request meet the guidance on the ICO website, we will inform the data subject in writing that we will erase their personal data in accordance with ICO guidelines. (Data Protection Officer)

7. Keep data safe and secure:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

a) All paper based material containing sensitive personal data must be held in lockable storage, whether on or off site. (ALL Staff)

b) Idsall School designates the Deputy Headteacher, Mr. D. Crichton ***and the*** Network Manager, Mr. A. Groucutt ***as the persons with responsibility for the security of IT systems.***

c) The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. (AG – Network Manager)

d) All users will use strong passwords which must be changed regularly, every 100 days. User passwords must never be shared. (AG – Network Manager)

f) Currently the screensaver auto locks are set to –

Network Administrative Accounts – 5mins of inactivity
Students Accounts – 5mins of inactivity
Staff Accounts on a Desktop PC – 10mins of inactivity
Staff Accounts on a laptop PC – 15 Minutes of inactivity

e) Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). (ALL Staff)

f) As a backup 'auto lock' will be enabled on all computers. (AG – Network Manager)

g) All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation. (AG – Network Manager)

h) Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (ie owned by the users, including personal cloud storage accounts and personal email accounts) must not be used for the storage of personal data. (ALL Staff)

i) Ensure that no unauthorised person can access data from computers that are no longer in use or subject to change of use. This will normally require the removal of all storage media from the device and safe disposal of any data stored on that media. (AG – Network Manager)

j) The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (AG – Network Manager)

k) The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. (AG – Network Manager)

l) If empty, staffrooms and offices should be locked. At the end of the working day, ensure all staffrooms and offices are locked. (ALL Staff)

NOTE: we are working towards replacing staffroom and office traditional key locks with self-

locking, push button, numerical code locks.

m) At the end of the working day the school buildings are also locked. (Site Management Team)

n) Personal data displayed on computer screens and manual files should be kept out of view of callers to the school/office. (ALL Staff)

o) Visitors signing into school at the reception desk should not be able to see the details of previous visitors.

NOTE: we are working towards a computer based system (eg using an ipad or tablet) to achieve this..

p) Any photographs of students on display around the school should only have the pupils forename displayed. (The exception to this is the Y11 Year Group photographs.)

q) Any documentation containing students' personal data (e.g. medical, assessment, SEND, targets) shall not be on display on walls or desks in staffrooms, offices or classrooms. Instead, they can be held in a labelled folder which can be locked in a staffroom or office or other lockable storage at the end of the working day.

7.1 Trips, visits and fixtures.

All trips, visits and fixtures are required to take information relating to any medical conditions of participants, consent forms from parents and for overseas trips; copies of passport and EHIC details. A senior member of staff, not participating in the event, will act as a contact for advice and guidance in the event of an incident. They too will need a copy of all the documents relating to the trip. These documents must be kept safe and secure at all times.

a) all documentation must be kept secure by the trip leader***. This will usually mean keeping the paperwork on their person or within sight during the trip or fixture as the information will need to be to hand in the event of an accident or medical emergency.***

b) In some cases, when the pack of documents is bulky, this may not be practical. In this event it is acceptable to keep the original documents locked in the accommodation/hotel safe (Trip Leader) ***and for staff members to carry a copy of the documents on an electronic device so long as:***

- The device is password/PIN/fingerprint protected.
- The device is kept on the staff's person at all times.
- Personal data transferred onto the device is supervised by the Network Manager
- Data is securely deleted from the device, under the supervision of the Network Manager, at the end of the trip or visit.

c) all documents containing personal data should be locked in a safe at the accommodation/hotel when the party return after an activity. (Trip Leader)

d) ***The senior member of staff, not participating in the event, who is acting as a contact for advice and guidance in the event of an incident, must keep the documents to hand and store them securely whilst off of school premises.*** (SLT – Trip Liaison)

e) On their return from a trip, visit or fixture all staff who participated shall return all documents to the Education Visits Coordinator (EVC), Mrs. M. Johnston***, for secure disposal and/or storage.***

7.2 Secure transfer of data and access out of school

Idsall School recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

a) Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and only when the criteria (b) and (c), below are met. (ALL Staff)

b) When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform. (ALL Staff)

NOTE:

- *VPN is available to use via staff laptops.*
- *Ericom Remote Access is available to use from all other devices.*

i. If secure remote access is not possible and personal data is stored on any portable computer system, USB stick, CD/DVD or any other removable media (ALL Staff)***:***

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

c) Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school. (ALL Staff)

d) Staff will be made aware of all practical measures to ensure the security of personal data, annually and through 'new staff' induction procedures. (DC – Data Protection Lead)

e) SIMS access will only be given to persons on contract to Idsall School or persons where a SLA exists requiring them to have SIMS access.

f) Trainee and associate teachers working and training temporarily at Idsall School will, as part of their induction process, be required to encrypt and password protect any removable media device that they intend to use whilst on placement at Idsall School. They must seek approval from the Network Manager. At the end of their placement they must present their removable media device to the Network Manager in order to ascertain and ensure all and any personal data has been removed from their device.

Sending information via email is by default not secure just like sending mail in the postal system the mail can be intercepted and read by anyone:

g) email attachments that contain personal data must be <u>password protected and encrypted</u> first before sending them, but then providing the recipient a password via <u>separate</u> communication channel for example a phone call.

8. Transfer of Data to Third Parties (inc. territories outside EEA)

- In order to facilitate the transfer of information to another school when a student transfers:

Note: *When a child is transferring from the school, the Headteacher must notify the Headteacher of the new school of any problems relating to school attendance that the child concerned had and of any other matters relating to the child's educational progress that he or she considers appropriate. Schools may supply personal data, or information extracted from such data, to other schools or another prescribed body if they are satisfied that it will be used in recording the student's educational history, monitoring the student's educational progress or developing the student's full educational potential.*

a) The S2S system will be used to transfer information about students to another school. (DL- Data Manager and LD - Admin Team Lead)

b) All generic files sent to DfE via S2S must be encrypted using 'Winzip'. (DL- Data Manager and LD - Admin Team Lead)

The S2S system allows schools and local authorities to securely share information, for example to:

- *transfer pupil records using the common transfer file protocol (CTF)*
- *update pupil details with the Learning Records Service (LRS)*
- *apply for and receive pupil unique learning numbers*
- *send and receive messages to and from other users within the S2S network*

Local authorities can also use S2S to report on the number of CTF transfers that have taken place in their region.

Log in

Access to S2S is only available via secure access, our secure point of entry for data transfer services.

Send files

To send information to another school or local authority, you must:

- *use the CTF naming protocols*
- *save the data in an encrypted folder or file*
- *send the file as a compressed folder*

Full instructions for saving, uploading and receiving files via S2S can be found in the guides for schools and local authorities.

- In what circumstances will personal data be disclosed to third parties, including the Department for Education, police, in legal proceedings, HSE, personnel etc.?

c) Idsall School, as the data controller, using a data processor (VH – Business Manager) ***will ensure, in a written contract, that:***

i. the processor only acts on instructions from the data controller; and

ii. it has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle.

Therefore a data processor involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller.

d) Idsall School will either seek consent or explicit consent for data sharing (LD – Admin Team Lead) ***where:***

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
- the individual would be likely to object should the data be shared without his or her consent; or
- the sharing is likely to have a significant impact on an individual or group of individuals.

or identify the lawful conditions that provide a basis for processing non-sensitive personal data, (DC – Data Protection Lead)***, these include when:***

i. The processing is necessary:
   - in relation to a contract which the individual has entered into;

   or
   - because the individual has asked for something to be done so they can enter into a contract.

ii. The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).

iii. The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

iv. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

v. The processing is in accordance with the "legitimate interests" condition.

8.1 Transfer of Data Abroad

An area of concern for many data controllers are the requirements necessary for the transfer of data abroad. There are special conditions that have to be met before transferring personal data outside the European Economic Area, where the importing country does not have an EU approved level of data protection law.

a) If there is a need to transfer personal data abroad Idsall School will ensure that at least one of the following conditions are met, (VH-Business Manager) ***in that the transfer is:***

- consented to by the data subject
- required or authorised under an enactment, convention or other instrument imposing an international obligation on this State
- necessary for the performance of a contract between the data controller and the data subject
- necessary for the taking of steps at the request of the data subject with a view to his or her entering into a contract with the data controller
- necessary for the conclusion of a contract between the data controller and a third party, that is entered into at the request of the data subject and is in the interests of the data subject, or for the performance of such a contract
- necessary for the purpose of obtaining legal advice
- necessary to urgently prevent injury or damage to the health of a data subject
- part of the personal data held on a public register
- authorised by the Data Protection Commissioner, which is normally the approval of a contract which is based on the EU model.

As the legislation on the transfer of data abroad is complex, it may be advisable for persons to contact the ICO in order to seek guidance on specific cases.

Exceptions to disclosure rule:

- ***Data can be disclosed when required by law***
- ***Data can generally be disclosed to an individual himself/herself or with his/her consent.***

Data Breaches

What is a personal data breach?

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.

a) Staff will be made aware of all practical measures to ensure the security of personal data, annually and through 'new staff' induction procedures. (DC – Data Protection Lead)

b) If a member of staff considers that a breach of personal data has occurred they will inform Mr. D. Crichton / Mrs. V. Hulme / Mr. A. Groucutt ***and complete sections 1 – 4 of the Personal Data – Breach Record (Appendix G) within 24hrs.*** (ALL Staff)

c) Mr. D. Crichton / Mrs. V. Hulme / Mr. A. Groucutt ***will complete sections 5 – 10 of the Personal Data – Breach Record (Appendix G). This may require further investigation to complete fully.***

d) If the data breach is deemed MINOR, the Breach Record will be printed and filed in the Breach Record folder held by Mr. D. Crichton***.***

e) If the data breach is deemed SERIOUS, the Data Protection Officer ***will be informed immediately and a meeting arranged within 48hrs to discuss the next steps. The Breach Record will also be printed and filed in the Breach Record folder held by*** Mr. D. Crichton***.***

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

f) If it is deemed necessary, the Data protection Officer ***will notify the ICO within 72hrs of the breach. In discussion with*** Mr. D. Crichton / Mrs. V. Hulme / Mr. A. Groucutt and the Headteacher, the DPO ***will also formulate the strategy for informing data subjects affected by the data breach.***

g) When reporting a breach to the ICO, the Data Protection Officer ***will provide:***

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- 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.

h) A regular meeting (at least once per term) between the *Data Protection Officer and Mr. D. Crichton / Mrs. V. Hulme / Mr. A. Groucutt* ***will be arranged in order to discuss the Breach Record and to review training and policy implications.***

Appendix A

Data Protection Statement for inclusion on relevant forms when personal information is being requested

The information collected on this form will be held by Idsall School in manual and in electronic format. The information will be processed in accordance with the Data Protection Act, 1988, the Data Protection (Amendment) Act, 2003 and the General Data Protection Regulation, coming into effect on 25th May 2018.

The purpose of holding this information is ….. *(School should insert the relevant information eg. for administration, to facilitate the school in meeting the student's educational needs etc.).*

Disclosure of any of this information to statutory bodies such as the Department for Education or its agencies will take place only in accordance with legislation or regulatory requirements. Explicit consent will be sought from Parents/Guardians or students aged 16 or over if the school wishes to disclose this information to a third party for any other reason.

Parents/Guardians of students and students aged 16 or over have a right to access the personal data held on them by the school and to correct it if necessary.

I consent to the use of the information supplied as described.

Signed Parent/Guardian: _____

Signed Student: _____

Appendix B: 6 lawful bases for collecting data:

1. **Consent from an individual** is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

You can process personal data without consent if it's necessary for:

2. **A contract with the individual**: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.

3. **Compliance with a legal obligation**: if you are required by UK or EU law to process the data for a particular purpose, you can.

4. **Vital interests**: you can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else.

5. **A public task**: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.

6. **Legitimate interests**: if you are a private-sector organisation, you can process personal data without consent if you have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests.

Private-sector organisations will often be able to consider the 'legitimate interests' basis in Article 6(1)(f) if they find it hard to meet the standard for consent and no other specific basis applies. This recognises that you may have good reason to process someone's personal data without their consent – but you must ensure there is no unwarranted impact on them, and that you are still fair, transparent and accountable.

Public bodies cannot generally rely on 'legitimate interests' under the GDPR, but should be able to consider the 'public task' basis in Article 6(1)(e) instead. However, you will need to be able to justify why the processing is necessary to carry out your functions – in essence, that it is proportionate and there is no less intrusive alternative. And, as always, you will need to ensure you are fair, transparent and accountable. Note that this basis cannot apply if you are acting for purposes other than your official functions – for example, if you are a hybrid body. In such circumstances you could still consider 'legitimate interests' as a potential basis, as long as the processing is otherwise lawful.

Appendix C **Conditions for processing special category data.**

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and we will publish more detailed guidance here once these provisions are finalised.

Appendix D

Privacy Notice (How we use pupil information)

Who we are
You already know that your school is called Idsall School, but we have to tell you that Idsall School is the organisation which is in charge of your personal information. This means that Idsall School is called the Data Controller.

The postal address of Idsall School is:

Idsall School
Coppice Green Lane
Shifnal
SHROPSHIRE, TF11 8PD

If you want to contact us about your personal information you can contact Mr. D. Crichton, Deputy Headteacher at school – by leaving him a letter at reception or send one by post. You can also contact the school's Data Protection Officer by email at ClerkOfGovernors@idsall.shropshire.sch.uk.

Why do we collect and use pupil information?

- Idsall School is under a legal obligation to collect the information or the information is necessary for us to meet legal requirements imposed upon us such as our duty to safeguard pupils.

We collect and use pupil information under the submission of the school census returns, including a set of named pupil records. This is a statutory requirement on schools under Section 537A of the Education Act 1996.

- It is necessary for us to hold and use your information for the purposes of our functions in providing schooling and so we can look after our pupils. This is a function which is in the public interest because everybody needs to have an education. This means we have real and proper reasons to use your information.

- We have a legitimate interest in holding and using your information because it is necessary in order to provide our pupils with education and pastoral care and connected purposes as outlined above.

- We will not usually need your consent to use your information. However, if at any time it appears to us that we would like to use your personal data in a way which means that we would need your consent then we will explain to you what we want to do and ask you for consent. This is most likely to be where we are involved in activities which are not really part of our job as a School, but we are involved because we think it would benefit our pupils. If you give your consent, you may change your mind at any time. If we think that you will not understand what we are asking then we will ask your parent or carer instead. Usually, we will involve your parents or carers even if you can make your own decision.

We use the pupil data:
- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to meet our safeguarding obligations
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:
- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)

- exclusions / behavioural information
- Assessment information (such as KS2, KS3, KS4, post-16)
- relevant medical information
- special educational needs information

Collecting pupil information
When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you / your parents or carers to provide it or whether there is a legal requirement on the school to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

Storing pupil data
We only keep your information for as long as we need to or for as long as the law requires us to. Most of the information we have about you will be in your pupil file. We usually keep this information until your 25th birthday unless you move to another school in which case we send your file to your new school. We have a policy which explains how long we keep information.

Who do we share pupil information with?
- Your new school if you move schools
- Disclosures connected with SEND – e.g. non-Local Authority professionals
- Organisations relating to the welfare and safety of pupils.
- School nurse
- School Counsellor
- CAMHS (Child and Adolescent Mental Health Service)
- Educators and Examining Bodies
- The Department for Education
- Shropshire County Council
- NHS
- Police, Fire and Rescue Service, Ambulance Service and other emergency or enforcement agencies

The information disclosed to these people / services will include sensitive personal information about you. Usually this means information about your health and any special educational needs or disabilities which you have. We do this because these people need the information so that they can support you.

Aged 14+ qualifications
For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications

Why we share pupil information
Our disclosure of your personal data is lawful for the following reasons:
- Idsall School is under a legal obligation to disclose the information or disclosing the information is necessary for us to meet legal requirements imposed upon us such as our duty to look after our pupils and protect them from harm. (We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013).
- It is necessary for us to disclose your information for the purposes of our functions in providing schooling. This is a function which is in the public interest.
- We have a legitimate interest in disclosing your information because it is necessary in order to provide our pupils with education and pastoral care and connected purposes as outlined above.
- It is in your vital interests for your personal information to be passed to these people or services.
- We will not usually need consent to disclose your information. However, if at any time it appears to us that we would need consent then this will be sought before a disclosure is made.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

What is different about pupils aged 13+?
Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Our pupils aged 16+
We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and

retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs. V. Hulme, Business Manager, Idsall School.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:
If you would like to discuss anything in this privacy notice, please contact:

- Mrs. V. Hulme, Business Manager, Idsall School

or

- Mr. D. Crichton, Deputy Headteacher, Idsall School

Appendix E

Privacy Notice (How we use school workforce information)

Why do we collect and use workforce information?

We process this information under:

- Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- Article 9(2)(b) processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

- We collect and use workforce information under the submission of the school workforce census return. Including a set of individual staff records, is a statutory requirement on schools and local authorities by virtue of regulations made under sections 113 and 114 of the Education Act 2005. (For further information: https://www.gov.uk/education/data-collection-and-censuses-for-schools)

Putting the school census on a statutory basis means that:

- although schools and local authorities must meet their obligations to data subjects under the Data Protection Act, they do not need to obtain consent for the provision of information from individual members of the workforce.
- schools and local authorities are protected from any legal challenge that they are breaching a duty of confidence to staff members.
- schools and local authorities must complete a return.

and includes a basis from Article 6, and one from Article 9 where data processed is special category data from the GDPR-from 25 May 2018

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, addresses, employee or teacher number, national insurance number, etc)
- special categories of data including characteristics information (such as gender, age, ethnic group, etc)
- contract information (such as start dates, hours worked, post, roles, salary and payroll information, etc)
- work absence information (such as number of absences and reasons including relevant medical information, etc)
- qualifications (and, where relevant, subjects taught)
- employment history and references

Why we collect and use this information
We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- to fulfil our “Caring about Sickness” (CAS) obligations
- inform the development of recruitment and retention policies
- enable individuals to be paid
- to support Safer Recruitment

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data for a period of time specified in the "retention schedule schools" document.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Mrs. V. Hulme, Business Manager, Idsall School

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:

- Mrs. V. Hulme, Business Manager, Idsall School

or

- Mr. D. Crichton, Deputy Headteacher, Idsall School

Appendix F

Costs related to a Data Access Request

Number of pages of information to be supplied	Maximum fee (£)
1-19	1.00
20-29	2.00
30-39	3.00
40-49	4.00
50-59	5.00
60-69	6.00
70-79	7.00
80-89	8.00
90-99	9.00
100-149	10.00
150-199	15.00
200-249	20.00
250-299	25.00
300-349	30.00
350-399	35.00
400-449	40.00
450-499	45.00
500+	50.00

If a subject access request does not relate to the educational record, we will respond within 20 working school days. The maximum charge that will apply is £10.00.

Appendix G

Personal Data - Breach Report

Report prepared by:		
Date:		
On behalf of		**Idsall School**
1	Summary of the event and circumstances	*When, what, who – summary of incident…*
2	Type and amount of personal data	*Title or name of documents. What personal data was included?*
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	*Has information been retrieved? When? Has the loss been contained?*
*ONCE COMPLETED - PLEASE PASS / EMAIL SECTIONS 1 – 4 to **either** D. Crichton / V. Hulme / A. Groucutt*		
Sections 5 – 10 below to be completed by D.Crichton / V. Hulme / A. Groucutt		
5	Procedures / instructions in place to minimise risks to security of data	*(communication, secure storage, sharing and exchange)*
6	Breach of procedure/policy by staff member	*Has there been a breach of policy?* *Has appropriate management action been taken?*
7	Details of notification to affected data subject Has a complaint received from Data Subject?	*Has the data subject been notified? If not, explain why not. What advice has been given to affected data subjects?*
8	Details of Data Protection training provided:	*Include date of last training prior to the incident by the staff member breaching security.*
9	Procedure changes to reduce risks of future data loss	
10	Conclusion	**Serious** / **Minor** *Likelihood of it happening again…*