



DATA PROTECTION & FREEDOM OF INFORMATION POLICY

This policy has been adopted by the Management Committee on:

Date adopted:	21 st November 2018
Signed:	
Next review due:	November 2020

Voyage Learning Campus (VLC) Data Protection & Freedom of Information Policy

To be read in conjunction with the following documents:

- ***VLC Data Security Plan***

- 1.1 The Voyage Learning Campus** collects, stores and processes personal information about staff, students, parents, Management Committee members, visitors and other individuals who come into contact with the school in accordance with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. The policy applies to all data, regardless of whether it is in paper or electronic format.
- 1.2 This information is gathered in order to enable it to provide education and other associated functions. In addition, there will be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. The policy should be read in conjunction with the VLC Data Security Plan (May 2017).
- 1.3 Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The VLC will renew this registration annually or as otherwise legally required. Schools also have a duty to issue a Privacy Notice to all students/parents; this summarises the information held on students, why it is held and the other parties to whom it may be passed on. A Data Collection Form is issued to all parents upon admission to the school highlighting the VLC Privacy Notice (appendix A) which is available on the VLC website.

2. Purpose

- 2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
- 2.2 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3. Roles and Responsibilities

This policy applies to all staff employed by the VLC and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Management Committee

The Management Committee has overall responsibility for ensuring that the VLC complies with all relevant data protection obligations.

3.2 **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is I-West and is contactable via i-west@bathnes.gov.uk, Telephone number 01225 395959

3.3 **Principal**

The Principal acts as the representative of the data controller on a day-to-day basis.

3.4 **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

3. **What is Personal Information?**

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

4. **Data Protection Principles**

- 4.1 The VLC will comply with the data protection principles of the GDPR specified in Article 5. These are that personal data must be

1. processed lawfully, fairly and in a transparent manner in relation to individuals
 2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 4.2 The VLC will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures. The concept of data protection by design will be a guiding principle in achieving the security of individual's data protection rights.
- 4.3 In all aspects of our work we will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of our work. The rights of the data subject as defined in Chapter iii of the GDPR are;
- a) The Right to be informed in a clear, concise and transparent manner
 - 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 related to automated decision making

5. General Statement

- 5.1 The school is committed to maintaining the above principles at all times. Therefore the school will:
- Inform individuals why the information is being collected when it is collected

- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
 - The VLC keeps electronic data indefinitely and is held securely on corporate systems
 - The VLC destroys based legacy data in a controlled manner using industry specialists
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

6. Response time in the application of legislation

- a) Subject Access Requests (SARs) whereby an individual may request information held by the VLC about themselves or a nominated individual on their behalf must be responded to within 1 month,
- b) Where the above is found to be complex or numerous an extension may be granted allowing an additional 2 months however the subject must be informed within 1 month of their request,
- c) No fee shall be charged for the above except where it is found to be excessive, repetitive or manifestly unfounded in accordance with article 12 of the GDPR,

Subject Access Requests (SARs) must be submitted in writing, either in a letter, email or fax to the Data Protection Officer. They should include the name of the individual, correspondence address, contact number and email address and details of the information required. If staff receive a SAR they must immediately inform the Schools Operations Manager

6.1 An individual when making a SAR is entitled to the following.

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

7. Data Retention

- 7.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
- 7.2 Except where a specified retention period has been defined in accordance with the purpose of the activity any period of retention is defined by the Voyage Learning Campus record retention schedule.

8. Complaints

- 8.1 Where an individual makes a complaint relating to the processing of their personal data or is unhappy with any response to an SAR, FOI or EIR (if appropriate) request they may request an internal review (IR) be conducted. Requests for an IR should be within 40 days of the original response. The responsibility for the conduct of an IR is with the Voyage Learning Campus who will discuss with the appointed DPO i-west. The VLC contact is Jemma Howells, Schools Operations Manager.
- 8.2 If an individual is unhappy with the outcome of the IR they have the right to appeal to the Information Commissioner's Office (ICO) for assessment, the ICO is contactable at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

9. Personal Data Breaches

- 8.1 The VLC will make all reasonable endeavors to ensure that there are no personal data breaches.
- 8.1 Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the DPO will be informed immediately and the Security Incident Management (SIM) process will be carried out. The SIM is designed to manage, investigate, report and provide 'Learning from Experience' (LFE) to avoid future incidents occurring.
- 8.2 In any case an incident must be reported no later than 24hours from identification, except where a malicious incident has occurred. The learning culture within the VLC will seek the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.
- 8.3 Where appropriate, we will report the data breach to the ICO within 72 hours.

9. Training

- 9.1 All staff and Management Committee members are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the VLC's processes make it necessary.

10. Monitoring and discipline

- 10.1 Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the VLC, in consultation with the Senior Leadership Team, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

11. Contacts

- 11.1 If you have any enquires in relation to this policy, please contact the school by letter or email to the School Operations Manager, Voyage Learning Campus, Oldmixon Crescent, Ashcroft House, Weston super Mare, BS24 9AX who will also act as the contact point for any subject access requests.

Email address: jemma.howells@voyagelearningcampus.org.uk

- 11.2 Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

▬

The Voyage Learning Campus is a data controller for the purposes of the General Data Protection Regulation (GDPR). We collect, hold and use personal information relating to our pupils and may also receive information about them from their previous school, local authority and / or the Department for Education (DfE). The information we hold is used to support teaching and learning, monitor and report on your child's progress, provide appropriate pastoral care and assess how well your child is doing.

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

- Personal information and contact details (such as name, unique pupil number, contact details and address)
- Characteristics (such as ethnicity, language, free school meal eligibility)
- Safeguarding Information (such as court orders and professional involvement)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Special Educational Needs information (such as category and needs type)
- Behavioural information (such as behaviour logs/incidents, exclusions, any alternative provision)
- Assessment and attainment (such as National Curriculum Assessment results, post 16 courses enrolled for and any relevant internal assessments and externally set tests and results)
- Medical information (such as doctors information –name and address, child health, medication, allergies and dietary requirements)
- For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.
- Details of any support received, including care packages, plans and support providers
- Health and Safety information (such as accidents, incidents and first aid records)
- Images, audio and video recordings (such as audio recording for exam entrants)

Why do we collect and use pupil information?

We use this personal data to:

- a) provide your child with an education
- b) support our pupils' learning and assist with personalised learning
- c) monitor and report on their progress and attainment
- d) to provide appropriate pastoral care
- e) to assess the quality of our services
- f) to comply with the law
- g) to ensure safety of pupils whilst in our care
- h) to facilitate home to school communication
- i) to meet the statutory duties placed upon us regarding data sharing

The lawful basis on which we use this information

Under the General Data Protection Regulation (GDPR), the lawful basis we rely on for processing pupil information is:

APPENDIX 1

- in accordance with the legal basis of Legal obligation: data collected for DfE census information
 - Section 537A of the Education Act 1996
 - the Education Act 1996 s29(3)
 - the Education (School Performance Information)(England) Regulations 2007
 - regulations 5 and 8 School Information (England) Regulations 2008
 - the Education (Pupil Registration) (England) (Amendment) Regulations 2013
- in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)
- in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function

The school must also comply with additional conditions where it processes special categories of personal information, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, health information and information about sex life or orientation. Data relating to criminal offences is also offered similar special protection. We do so in accordance with applicable law (including with respect to safeguarding or employment) or by explicit consent.

Consent will be required under exceptional circumstances where the processing of data does not fall under any other lawful basis. Under the provision consent must be

- Freely given
- State the exact purpose for processing data
- Provided under a clear, affirmative action
- Provided separately to agreement to any other terms and conditions

Consent can be withdrawn at any time, at which processing of the data will be halted. If you would like to withdraw consent, please contact the Schools Operations Manager.

Collecting pupil information

We ask parents / carers to complete student agreement forms upon starting at the school. Data Collection Sheets are sent to new starters to ensure the information we receive from other schools is accurate and complete. Pupil information is checked for accuracy at the beginning of every new academic year using Data Collection Sheets. Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

If your child has or develops a medical condition that requires medication to be taken at school, medication forms will be issued for completion.

Personal data held by us is processed by appropriate members of staff for the purposes for which the data was provided. We take appropriate technical and organisational steps to ensure the security of personal data about individuals around use of technology and devise and access to school systems. We do not transfer data outside of the European Economic Area unless we are satisfied that the personal data will be provided an equivalent level of protection.

Some of our systems are provided by third parties e.g. hosted databases, school websites or cloud storage providers. All of our providers are asked to provide their privacy notices to ensure they are compliant with GDPR. A central log of all systems which are provided by third parties are kept and monitored by the Schools Operations Manager.

APPENDIX 1

We also receive Common Transfer Files from previous schools via the DfE's Secure Access site and the Local Authority AnyComms system.

Storing pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information regarding our data retention schedule and how we keep your data safe, please visit **our website**.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- schools where a pupil may be dual registered
- North Somerset Council
- Youth support services (pupils aged 13+)
- the Department for Education (DfE)

Why we share pupil information

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

Currently we share information with:

1. **Department of Education**

We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information)(England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework. For more information, please see 'How Government uses your data' section.

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy. (for example how certain subject choices go on to affect education or earnings beyond school)

APPENDIX 1

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>

2. **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.

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

Sharing

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfe-external-data-shares>
To contact DfE: <https://www.gov.uk/contact-dfe>

3. **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.

APPENDIX 1

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once he/she reaches the age 16.

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

Data is securely transferred to the youth support service via a secure file transferring system and is stored within local authority software.

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

4. **Connecting Care**

Connecting Care brings together information sharing across health and local government in the south west via an online portal. It is not new sharing – it is simply sharing done in a more effective way.

North Somerset Council is a partner in Connecting Care, a project which links social care information with health information. Schools cannot access Connecting Care but they may share information that could appear on Connecting Care.

The Connecting Care Local Record is a new way for staff who are directly involved in a child's care to share relevant information about their care in a way that is secure, controlled, consistent and efficient. It allows health and local council staff who are directly involved in a child's care access to a summary of existing records, such as those held by the GP, hospital or social care provider. Staff who are directly involved in a child's care, will only access their record with a legitimate reason, and if they can, they will ask your permission before they look at it.

The Connecting Care Record will contain information on:

- Who is involved in a child's care
- Any allergies they have
- Medications
- Recent appointments (but only whether they were attended, this will not include any information about what was discussed at that appointment)
- Diagnoses

The Connecting Care record will not contain information about conversations with the GP or any information on sensitive subjects such as sexual health. Staff who have a responsibility for designing services to improve children's general well-being will also

APPENDIX 1

have access to relevant information from the record. The detail that staff can see is linked to the job they do. If for their job they don't need to see specific information, they cannot see it.

If you require further information about Connecting Care please contact PALS 0800 073 0907, or visit <https://www.bristolccg.nhs.uk/about-us/how-we-use-your-information/connecting-care/>

5. **South West Partnership**

We use South West Partnership to offer work experience opportunities to students in years 10 and year 11. We provide them with

- The names of pupil's
- The date of birth of the pupil

6. **North Somerset Community Partnership CIC**

North Somerset Community Partnership CIC provides immunisations for school aged students. We provide them with

- The names and addresses of pupils
- The date of birth of the pupil

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 Jemma Howells, VLC Schools Operations Manager or our Data Protection Officer by emailing i-west@bathnes.gov.uk

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
- a right to seek redress, either through the ICO, or through the courts

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:

- Schools Operations Manager, Voyage Learning Campus, Oldmixon Crescent, Weston super Mare, BS24 9AX 01934 836298
- www.n-somerset.gov.uk

LOCAL AUTHORITY (LA) FULL PRIVACY NOTICE

Children and young people: information held by local authorities

The Data Protection Act 1998: How we use your information

We use information about children and young people to enable us to carry out specific functions for which we are responsible. We also use this personal data to derive statistics which inform decisions we make (e.g.) regarding the funding of schools, assessing their performance and to set targets for them.

We are legally obliged to share information with other agencies (e.g. Police, Health, schools) when there are **safety concerns** about children.

Since the implementation of the Education and Inspections Act 2006, and specifically the duty for local authorities to provide a sustainable travel to schools strategy, North Somerset Council has been involved with assessing pupil travel needs and reviewing transport infrastructure to all its schools. **School mode of travel** information, collected from schools, is shared with the School Travel Advisers in the North Somerset Council Sustainable Travel Team.

The LA uses information from schools and its own data to annually develop a risk indicator for all young people aged 11-17 to identify those young people who are at greatest risk of becoming not in education, employment or training (NEET). The **RONI (Risk of NEET Indicator)** and the schools data on which it is based will be shared with all educational establishments funded by the Education Funding Agency (EFA) with an 11-17 cohort in North Somerset.

Information will be shared as part of the statutory duty of LAs to provide the **September Guarantee**: working with their partners to provide education and training to all 16- and 17-year-olds and to support young people to find something suitable to meet their needs; and the **Raising of the Participation Age Strategy**: to ensure that all young people are offered appropriate learning and training opportunities up to the age of 19.

Information will be shared with the DfE in accordance with the NCCIS Management Information Sharing Requirement which is annually reviewed and published – See link below for 2017/18

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/575941/NCCIS_Management_Information_Requirement_2017_to_2018_Final.pdf

The LA will use attendance, exclusion and data relating to behaviour, collected from schools along with its own data, to assist with the identification (and subsequent monitoring) of children or young people in families who meet the criteria of a High Impact Family. Families (including children or young people) meeting the criteria will be offered a variety of services and support dependent on their individual needs. **The High Impact Families Programme** represents the local element of the Government's national initiative to turn around the lives of 400,000 multi-need families by 2020. The aim is that the children in these families have the chance of a better life.

Appendix 2

The LA will use information about its **school workforce** for research and statistical purposes, and to evaluate and develop education policy and strategies. The statistics are used in such a way that individual staff cannot be identified from them. The LA may also use it to support and monitor schools regarding sickness and recruitment of staff.

Local Health Services, (including Clinical Commissioning Groups) use information about pupils for research and statistical purposes, to develop, monitor and evaluate the performance of local health services. These statistics will not identify individual pupils. It is necessary for certain health information about children (e.g. such as their height and weight) to be retained for a certain period of time (designated by the Department of Health) and requires these Local Health Services to maintain children's names and addresses for this purpose. Local Health Services may also provide individual schools and LAs with aggregated health information which will not identify individual children. The LA may supply pupil details to assist with National Immunisation Programmes or other national health monitoring initiatives (e.g. to North Somerset Community Partnership Community Interest Company).

- Email Contact: Kate.Tregale@swcsu.nhs.uk
Postal Contact: Information Governance Manager, South West Commissioning Support Unit, South Plaza, Marlborough Street, Bristol BS1 3NX.

Connecting Care

Connecting Care brings together information sharing across health and local government in the south west via an online portal. It is not new sharing – it is simply sharing done in a more effective way.

Your LA is a partner in Connecting Care, a project which links social care information with health information.

The Connecting Care Local Record is a new way for staff who are directly involved in a child's care to share relevant information about their care in a way that is secure, controlled, consistent and efficient. It allows health and local council staff who are directly involved in a child's care access to a summary of existing records, such as those held by the GP, hospital or social care provider. Staff who are directly involved in a child's care, will only access their record with a legitimate reason, and if they can, they will ask your permission before they look at it.

The Connecting Care Record will contain information on:

- Who is involved in a child's care
- Any allergies they have
- Medications
- Recent appointments (but only whether they were attended, this will not include any information about what was discussed at that appointment)
- Diagnoses

The Connecting Care record will not contain information about conversations with the GP or any information on sensitive subjects such as sexual health. Staff who have a responsibility for designing services to improve children's general well-being will also have access to relevant information from the record. The detail that staff can see is linked to the job they do. If for their job they don't need to see specific information, they cannot see it.

If you require further information about Connecting Care please contact PALS 0800 073 0907, or visit <https://www.bristolccg.nhs.uk/about-us/how-we-use-your->

[information/connecting-care/](#)

Youth Support Services - The LA has a targeted youth support service for young people resident in North Somerset, aged 13-19 (up to age 25 for care leavers, or those with a special education need or disability).

For pupils aged 13 and over, schools are legally required to pass certain information to North Somerset Council (NSC) to enable NSC to track participation in education and training up to the age of 19 with their youth support services. The school must provide; the name, date of birth, address and name of the pupil's parent(s)/(guardians) and any further information relevant to the support services' role.

The NSC youth support services share some of the information collected with the Department for Education (DfE) to enable them to: produce statistics, assess our performance, determine the destinations of young people after they have left school or college and to evaluate Government funded programmes.

The NSC youth support services pass on some of the information they collect to other Local Authorities, for example when a young person is resident in a different LA, but is participating in education or training within NSC. Information may also be shared with providers who secure Government funding to support young people's participation or employment. This may include name, contact details, aspirations, participation history and any information that may support participation. Any information sharing will be supported by data sharing agreements and operate within Data Protection and Information Governance guidelines.

If you require more information about how the DfE store and use your information then please go to the following website:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

NSC and the Department of Work and Pensions (DWP) have a joint data sharing protocol which enables us to share data.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266788/Working_together_to_support_Young_People_NEET_.rtf

Post 16 Providers attended by North Somerset Learners - The school (Academy) or the LA will share demographics and personal characteristics of a young person with post 16 providers that have a progression route for North Somerset learners. These providers may be able to offer choices to the young person which could improve their life chances, enabling them to participate and make a positive contribution. The information will also be shared as part of the September Guarantee process and Raising of the Participation Age Strategy.

We hold information about young people living in our area, including about their education and training history. This is to support the provision of their education up to the age of 20 (and beyond this age for care leavers or those with a special education need or disability). Education institutions and other public bodies (including the Department for Education (DfE), police, probation and health services) may pass information to us to help us to do this (Covered Under the Education and Skills Act 2008, parts 1 and 2).

We share some of the information we collect with the Department for Education (DfE) to enable them to; produce statistics, assess our performance, determine the destinations of

Appendix 2

young people after they have left school or college and to evaluate Government funded programmes.

We may also share information with post-16 education and training providers to secure appropriate support for them. We may also share data with education establishments which shows what their pupils go on to do after the age of 16.

Online information, advice and support on a range of issues affecting young people can be found on the Gov.UK Education and Learning page at: <https://www.gov.uk/browse/education/find-course>

For children under 16, a parent or guardian can ask that no information other than their child's name, address and date of birth (or their own name and address) be passed to a local authority or youth support services provider. This right transfers to the child on their 16th birthday. Pupils and/or a parent/guardian will need to inform the school if this is what they wish.

Weston College

- Email contact: fiona.waters1@weston.ac.uk
Postal Contact: Fiona Waters, College Registrar, Weston College, Knightstone Road, Weston-super-Mare, North Somerset, BS23 2AL

The DfE may share individual level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether the DfE releases this personal data to third parties are subject to a robust approval process and are 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 level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

- <http://www.n-somerset.gov.uk/my-council/data-protection-foi/school-privacy-notice/school-privacy-notice/>
- <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

If you would like a copy of the information that we hold and share about you (subject access request) then please follow the below link for details of the process you will need to follow: http://www.n-somerset.gov.uk/Your_Council/Freedom_of_information/Pages/Freedom-of-information.aspx

DEPARTMENT OF EDUCATION PRIVACY NOTICE

Data Protection – how the Department for Education (DfE) collects and shares research data

Privacy Notices

Data protection: how the DfE shares pupil and workforce data

How and when we share the pupil, child and workforce data we collect for research and statistical purposes.

Contents

1. [Data we collect](#)
2. [When we share data](#)
3. [Longitudinal education outcomes study](#)

Data the DfE collects

The Department for Education has legal powers to collect the pupil, child and workforce data that schools, local authorities and awarding bodies hold.

For more information on the legislation which allows this, see:

- [section 114 of the Education Act 2005](#)
- [section 537A of the Education Act 1996](#)
- [section 83 of the Children Act 1989](#)

This data forms a significant part of our evidence base. We use it:

- in [school performance tables](#)
- in [adoption scorecards](#)
- in [statistical first releases](#)
- to evaluate and inform educational policy
- to assess funding to local authorities and schools

We hold pupil-level data in the [national pupil database](#).

When the DfE shares data

Pupil data

The law allows us to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- companies who are producing products connected with promoting the education or wellbeing of children in England
- other government departments and agencies

See the [Education \(Individual Pupil Information\) \(Prescribed Persons\) \(England\) Regulations 2009 SI 2009/1563](#).

We can share pupil-level information we've collected from:

- regular data returns from schools and local authorities

- the national pupil database (NPD)

Before we grant access to individuals requesting data from the NPD, they must comply with the terms and conditions imposed under contractual arrangements, as well as a rigorous request approval process.

See [requests for NPD data made by third parties since April 2012](#).

See [guidance on applying for data from the NPD](#).

We may also share selected individual pupil data with the [Office for National Statistics](#) for the development of population and migration statistics.

We may decide to share pupil and children's information with third parties on a case-by-case basis where:

- we're satisfied that to do so would be in accordance with the law and the [Data Protection Act \(1998\)](#)
- we consider that the disclosure would promote the education or wellbeing of children

See [guidance to schools and local authorities](#) on the legal requirement to provide privacy notices to staff, parents and pupils to explain how their personal data will be collected and used.

Workforce data

The [Education \(Supply of Information about the School Workforce\)\(No.2\)\(England\) Regulations 2007](#) allows us to share workforce data with the following third parties:

- [Local Government Association](#)
- [HM Chief Inspector of Education, Children's Services and Skills \(Ofsted\)](#)
- [National Audit Office](#)
- [Office of Manpower Economics](#)
- [Administrator of the Teachers' Pension Scheme](#)
- local authorities
- [Service Children's Education](#)
- school proprietors
- independent researchers where disclosure may be expected to be of public benefit

Longitudinal education outcomes study

The [privacy notice for the 'Longitudinal education outcomes study'](#) explains how the government handles and shares NPD data as part of the study. The study compares students' level of education to their level of employment and earnings in later life.