



The Clere School

GDPR Data Protection Policy

Date of last review:	June 2024
Date of policy issue:	June 2025
Statutory/Discretionary: Statutory	Statutory
Name of Headteacher approving this policy:	Mrs Jayne McLaren
Name of Chair of Governors approving this policy:	Mr Garry Parker
Date for next review of this policy:	June 2026

Contents

Purpose & Data Protection Principles	Page 2
GDPR Commitments	Page 3
Complaints	Page 4
Appendix 1 – Procedures for Responding to SARs	Page 5
Appendix 2 – Privacy Notice Students and Parents	Page 7
Appendix 3 – Privacy Notice Staff and Governors	Page 11
Appendix 4 – Privacy Notice Community Provision	Page 14
Appendix 5 – Data Breach Reporting Form	Page 17

The Clere School collects and uses personal information (referred to in the UK General Data Protection Regulation (UK GDPR) as personal data) about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The Assistant Head Teacher is the Data Protection Officer at the school.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all students/parents and staff. These summarise the personal information held about students and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the UK GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information / data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, and an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The UK GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Lawfulness, fairness and transparency. Personal data shall be processed lawfully, fairly and in a transparent manner. In order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the UK GDPR. These include (amongst other relevant conditions) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority exercised by the school.

Where the special categories of personal data are processed, this shall include (amongst other relevant conditions) where processing is necessary for reasons of substantial public interest. When processing personal data and special category data in the course of school business, the school will ensure that these requirements are met where relevant.

2. Purpose limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes). The school will only process personal data for specific purposes and will notify those purposes to the data subject when it first collects the personal data or as soon as possible thereafter.

3. Data minimisation. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive. Personal data which is not necessary for the purpose for which it is obtained will not be collected.

4. **Accuracy.** Personal data shall be accurate and where necessary, kept up to date; Personal data should be reviewed and updated as necessary and should not be retained unless it is reasonable to assume that it is accurate. Individuals should notify the school of any changes in circumstances to enable records to be updated accordingly. The school will be responsible for ensuring that updating or records takes place where appropriate.

5. **Storage limitation.** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The school will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected and will take reasonable steps to destroy or erase from its systems all data which is no longer required.

6. **Integrity and confidentiality.** Personal data shall be processed in a manner that ensures appropriate security of the personal data and which includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Duties

Personal data shall not be transferred to a country or territory outside the UK and the European Union (EU)/European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller.
- Inform individuals of the contact details of the Data Protection Officer.
- Inform individuals of the purposes that personal information is being collected and the basis for this.
- Inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the UK and the EU/EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information.
- Inform individuals of their data subject rights.
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept.
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)

- Ensure that personal information is not transferred outside the UK and the EU/EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Disposal of Personal Data

The school will dispose of personal data in a way which protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) as appropriate.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Headteacher or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the contact point for any queries.

Appendices:

Appendix 1 – Procedures for Responding to Subject Access Request
 Appendix 2 – Privacy Notice – Students & Parents
 Appendix 3 – Privacy Notice – Staff & Governors
 Appendix 4 – Privacy Notice - Community
 Appendix 5 – Data Breach Reporting Form

Appendix 1

PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS

Rights of access to information

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

1. Under the General Data Protection Regulation 2018 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Student Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the General Data Protection Regulation 2018.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

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

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The school may make a charge for the provision of information, dependant upon the following:
 - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
 - Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
 - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.
 - If the information is to be sent by registered post then a charge of up to £5 will be required to provide it.
5. The response time for subject access requests, once officially received, is 30 days (**not working or school days but calendar days, irrespective of school holiday periods**). However, the 30 days will not commence until after receipt of fees or clarification of information sought.

6. The General Data Protection Regulation allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure.**
7. Third party information is that which has been provided by another, such as the Police, Local Authority or Health Care professional. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings, except as required by law.
9. If there are concerns over the disclosure of information then additional advice should be sought.
10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.
13. If the cost limit for complying with a request or a linked series of requests from the same person or group is set to exceed £450 a request can be refused. This is to ensure that a request does not cause a drain on time, energy and finances to the extent that they negatively affect our normal public functions.

Complaints

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 Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Appendix 2

PRIVACY NOTICE STUDENTS & PARENTS (How we use personal information)

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

- Personal information (such as name, unique student 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) and exclusions
- Assessment information
- Modes of travel
- Relevant medical, special educational needs and behavioural information
- Post 16 learning information
- Information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and child Protection Plan information)
- Episodes of being looked after (such as important dates, information on placements)
- Outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- Adoptions (such as dates of key court orders and decisions)
- Children in care (such as their activity and what type of accommodation they have)
- Special education needs information

Why do we collect and use personal information?

We collect and use personal information:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services and how well our school is doing
- to provide statistical forecasting and planning
- to comply with the law regarding data sharing
- to evaluate and improve our policies on children's social care

The Lawful basis on which we use this information

We collect and process information about children in our care and children to whom we provide services under the following lawful basis:

- Compliance with a **legal** obligation
- Performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.
- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

The General Data Protection Regulation allows us to collect and use student information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the data subject and the vital interests of the data subject or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children's Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Storing personal data

We hold student data in accordance with our Retention Schedule.

Who do we share student information with?

We routinely share student information with:

- Schools and colleges
- our local authority
- the Department for Education (DfE)
- External agencies such as the police and Children's Services

Aged 14+ qualifications

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

Why we share student information

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

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.

Why we share student information – children in need and children looked after

Department for Education (DfE) - We share children in need and children looked after data with the Department on a statutory basis, under Section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.

This data sharing helps to develop national policies, manage local authority performance, administer and allocate funding and identify and encourage good practice.

We do not share information about our children in need or children looked after with anyone without consent unless the law and our policies allow us to do so.

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>.

Children looked after: <https://www.gov.uk/guidance/children-looked-after-return>

Children in need: <https://www.gov.uk/guidance/children-in-need-census>

Youth support services

What is different about students aged 13+?

Once our students reach the age of 13, we also pass student 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 / student once they reach the age 16.

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

The National Student Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students 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 students 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 Students) (England) Regulations 2013.

To find out more about the student 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-student-database-user-guide-and-supporting-information>.

The department may share information about our students 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 student 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 student information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-student-database-requests-received>

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

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. Detail on how to make a request for your personal information, or be given access to your child's educational record are attached at Appendix 1.

You also have the right, subject to some limitations 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 finance@clere.school

Appendix 3

PRIVACY NOTICE STAFF & GOVERNORS (How we use employee information)

Why do we collect and use personal information?

We collect and use personal information:

- Enable the development of a comprehensive picture of the workforce and how it is deployed.
- Inform the development of recruitment and retention policies.
- To be able to process payroll so employees can be paid.
- To ensure the safeguarding of the students
- To ensure the welfare of our employees
- To comply with the law regarding data sharing

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

- Personal information (such as name, employee or teacher number, national insurance number, DOB and address)
- Special categories of data including characteristics information such as gender, age, ethnicity, language, nationality, country of birth
- Contract information such as start dates, hours worked, post, roles and salary information
- Work absence information such as number of absences and reasons.
- Qualification and where relevant, subjects taught.
- Relevant medical information.
- Performance Management information.

The General Data Protection Regulation allows us to collect and use staff information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the data subject and the vital interests of the data subject or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children's Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010.

The lawful basis for collecting and using staff information for general purposes are:

- 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.
- Compliance with a **legal** obligation
- Performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.
- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Data security and storage of personal data

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked briefcases. The use by staff of removable media eg USB sticks is not permitted
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are automatically reminded to change their passwords at regular intervals
- Staff and governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

Who do we share employee information with?

We routinely share employee information with:

- Our local authority
- the Department for Education (DfE)
- prospective employees via references

Why we share employee information

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

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.

Data Collection Requirements

The DfE collects and processes personal data relating to staff that work in state funded schools. 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 of well-being of children of the effective deployment of school staff 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 employee 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>

To contact DfE: <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 them that we hold. Detail on how to make a request for your personal information, or be given access to your record are attached at Appendix 1.

You also have the right, subject to some limitations 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 finance@clere.school

Appendix 4

PRIVACY NOTICE FOR COMMUNITY PROVISION – (How we use personal information)

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

Adults - Gym, studio classes and lettings

- Personal information (such as name, address, phone numbers and email addresses)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Bank sort codes and credit card details
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical, special educational needs and behavioural information
- Post 16 learning information
- Information relating to episodes of being a family in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and child Protection Plan information)
- Special education needs information

Why do we collect and use personal information?

We collect and use personal information:

- to administer healthy living activities
- to monitor and feed-back on participants progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to enable statistical forecasting and planning
- to comply with the law regarding data sharing
- to evaluate and improve our policies on social care for children & adults

Children – Nursery and Out of School Care

- Personal information (such as name, unique child number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth)
- Attendance information (such as sessions attended, number of absences and absence reasons) and exclusions
- Assessment information
- Relevant medical, special educational needs and behavioural information
- Information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and

child Protection Plan information)

- Episodes of being looked after (such as important dates, information on placements)
- Outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- Adoptions (such as dates of key court orders and decisions)
- Care leavers (such as their activity and what type of accommodation they have.
- Special educational needs information
- Medical records including hospital reports, medicine records and accident records

Why do we collect and use personal information?

We collect and use personal information:

- to support early years foundation stage development
- to monitor and report on a child's progress
- to provide appropriate pastoral care
- to assess the quality of our services and how well our service is doing
- to provide statistical forecasting and planning
- to comply with the law regarding data sharing
- evaluate and improve our policies on social care for children & adults

The Lawful basis on which we use this information

We collect and process information about children in our care and children to whom we provide services under the following lawful basis:

- Compliance with a **legal** obligation
- Performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.
- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

The General Data Protection Regulation allows us to collect and use information with consent of the data subject, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of a data subject or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the data subject and the vital interests of the data subject or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Children's Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010. Early Years Statutory Framework.

We collect and process information about adult service receivers, children in the care of our Nursery and Out of School Club provision.

Collecting personal information

Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. Where we are using your personal information only on the basis of your permission you may ask us to stop processing this personal information at any time.

Data security and storage of personal data

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked briefcases. The use by staff of removable media eg USB sticks is not permitted
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are automatically reminded to change their passwords at regular intervals

Who do we share information with?

We routinely share information with:

- our local authority
- external agencies such as the police and Children's Services

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

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>.

Children looked after: <https://www.gov.uk/guidance/children-looked-after-return>

Children in need: <https://www.gov.uk/guidance/children-in-need-census>

Appendix 5

DATA BREACH REPORTING FORM

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	
IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected?	

(e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
Form Completed by	
Position	
Date	