POLICY INFORMATION **STATUTORY**

Name of Policy/Procedure:	**Data Protection Policy – GDPR inc Staff and Student Privacy Statements**
Current version date:	Autumn Term 2024
Review cycle:	The policy will be reviewed in the light of operating experience and/or changes in legislation
Next review date:	as above

Adopted by the Governing Body of Ruskin Community High School

Signed:

Reviewed by	**Date**	**Approved**
DUROSE	March 2018	
Athene Atkinson	Autumn Term 2020	No change n/a
Hazel Goodwin – no change	Autumn Term 2021	FGB 22/11/2021
Hazel Goodwin	Autumn 2023	FGB 29/11/2023
Hazel Goodwin	Autumn 2024	FGB 26/11/2024

Aims

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with 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.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Scope of the Policy

Personal information - is any information relating to an identified, or identifiable, individual.

Special categories of personal data – Personal data which is more sensitive and so needs more protection, including information about an individual's

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics – where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing - is anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject – the identified or identifiable individual whose personal data is held or processed.

Data controller – A person or organisation that determines the purposes and the means of processing of personal data.

Data processor – A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller
Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is the data controller.

The school is registered with the ICO and will renew this registration annually or as otherwise legally required. Ruskin Community High School registration number **ZAO85156**.

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

Governing board
The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

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, 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 Hazel Goodwin and is contactable via Ruskin Community High School, Ruskin Road, Crewe CW2 7JT.

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

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

Data Protection Principles

The GDPR is based on data protection principles that our school must comply with:

1. Data must be processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed

6. Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

Collecting personal data
Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

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.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

Sharing personal data
We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – especially in relation to safeguarding where there is a legal obligation, or it is the public interest.

- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Access to personal information:
Employees, students and others have the right of access to any personal information that is being kept about them. A request to access personal data must be made in writing to the Headteacher.

Privacy Notices:

The school publishes a privacy notice on our website, which provides information about how and why the school uses personal data. (**See Appendix 3 and 4 for statements)**

The privacy notice is reviewed at regular intervals to ensure it reflects current processing.

The school issues privacy notice to parents/carers and staff before, or as soon as possible after, any personal data relating to them is obtained.

The school does not allow the recording of meetings on devices, without the written and expressed permission of all parties involved in the meeting.

CCTV
The school has CCTV in order to:

- Protect the school buildings and assets
- To increase personal safety of staff, students and visitors
- To reduce the fear of crime
- To support the Police in order to deter, detect, apprehend and prosecute offenders

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Access is restricted to those staff who operate the system or make decisions relating to how the images should be used.

This is further detailed in the CCTV Policy and Procedure.

Photographs and Electronic Images

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, banners advertising the school etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages including Facebook and Twitter

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Please note that website can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Where parents/carers have opted out, we take steps to ensure that the image is not identifiable in any of our materials.

Photographs published on the website, or elsewhere that include students will be selected carefully. Photographs taken by on the school camera by staff on school visits may be used in the curriculum, and displayed within the school to illustrate the work of the school except in cases where the parent/carer has opted their child out.

Students must not take, use, share, publish or distribute images of others without their permission.

If it is found that cameras or camera phones have been misused, the school will follow its usual disciplinary procedures.

Biometric recognition systems

Where we use student's biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students will be given a pin number and they can use the cash machine to pay into their account.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Email

It is recommended that the sending of personal and confidential data by email is secured by using a trusted network or by encrypting the data. At Ruskin we use Egress to send confidential information to external agencies.

Cheshire East Council will send emails via the Egress system. An individual will need to register to open and reply to the email. This system can be used to send encrypted emails.

The S2S system is a secure way in which to transmit personal data from school to school.

Information Security
All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. The use of computer passwords is a requirement of the school to avoid unauthorised access.

Staff MUST lock computer screens when away from their desk.

Data security and storage of records
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.

Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.

The school provides remote access when working from home. The connection is encrypted, and staff are not allowed to copy files from the system or to their personal printers at home.

Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policy for ICT and equipment)

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of records

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.

For example, we will use a confidential shredding company for paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Training
Data protection training is part of the school induction process.

Subject access requests and other rights of individuals
Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Parental requests to see the educational record
The will only apply to Ruskin as a maintained school.

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time (if the data does not fall under a different GDPR category)
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

(Internal Procedure)
Handling a subject access request:

The policy applies to personal information created or held by the school.

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.

Any individual has the right of access to information held about them. However, with students, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request.

A request for personal information held about a child requires consent if the child is able to understand (in broad terms) what it means to make a request and interpret the information. If the school is confident the child understands their rights, then the response will be to the child rather than the parent.

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 student. Evidence of the identity can be established by requesting for example:

- Passport
- Driving licence
- Utility bills with the current address
- Birth / marriage certificate
- P45/P60
- Credit card or Mortgage statement

The Headteacher should discuss the request with the student and take their views into account when making a decision. A student with competency to understand can refuse to consent to the request for their records. Where the student is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the student.

The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained.

Any information which may cause 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, or information relating to court proceedings.

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

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.

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.

If the student can understand his/her rights, then the school will respond to the student rather than the parent.

Further information can be found in:
Subject Access Code of Practice, ICO

Links to other policies and documents:

- Privacy Notices: Information about students in secondary schools and student referral units
- Privacy Notices: Staff
- Freedom of Information
- Acceptable Use of ICT and Equipment
- Social Media Policy
- E-Safety Policy (Staff)
- CCTV Policy
- Retention of Records Guidelines

Appendix 2: Personal data breach procedure
This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The DPO will alert the Headteacher and the Chair of Governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in Admin shared drive.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on Admin area.

The DPO and Headteacher will meet to review what happened and what measures can be taken to prevent it happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

For example:

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.

• In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 3 Privacy Notice Staff

Privacy Notice (How we use workforce information)

Ruskin Community High School / Cheshire East Local Authority is the Data Controller for the use of personal data in this privacy notice.

The categories of school information that we process

These include:

- personal information (such as name, date of birth, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group, nationality, country of birth, disability)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications and employment records (and, where relevant, subjects taught, work history, job titles, working hours, training records, professional memberships)
- Contact details
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, tax status
- DBS and personal information on the Single Central Record for safeguarding purposes
- Recruitment information, including copies of right to work documentation, references and other information included in an application form or cover letter as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- OHU referrals
- Outcomes of any disciplinary and/or grievance procedures
- Photographs
- Biometrics
- CCTV footage
- Data about your use of the school's information and communications system
- Risk assessments
- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we collect and use workforce information

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
e) improving the management of workforce data across the sector
f) allowing better financial modelling and planning
g) enabling ethnicity and disability monitoring; and
h) supporting the work of the School Teachers' Review Body

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

1. for the purposes of Category information in accordance with the legal basis of Processing shall be lawful only if and to the extent that at least one of the following applies:

    1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    2. 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;

    3. processing is necessary for compliance with a legal obligation to which the controller is subject;

    4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    5. 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;

In addition, concerning any special category data:

- conditions: Race, ethnicity, religious beliefs, sexual orientation and political opinions of GDPR - Article 9
- conditions: Trade union membership opinions of GDPR - Article 9
- conditions: Health, including any medical conditions, and sickness records opinions of GDPR - Article 9

Collecting workforce information

We collect personal information via recruitment application packs and staff forms.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. We create and maintain an employment file for each staff member, both electronic and on SAM. The school is phasing out paper records. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Records Management Policy which can be found in the Staff Handbook.

Who we share workforce information with

We routinely share this information with:

- our local authority (where applicable)

- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll, HR software,
- Pensions
- Our auditors
- the Department for Education (DfE). 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:
    - the arrangements in place to store and handle 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

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

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

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:
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.

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

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 the School Business Manager.

Depending on the lawful basis above, you may also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

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/

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the School Business Manager.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in November 2023.Contact If you would like to discuss anything in this privacy notice, please contact the School Business Manager.

How government uses your data

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

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

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.

Sharing by the department

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.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter
To contact the department: https://www.gov.uk/contact-dfe.

Contact
If you would like to discuss anything in this privacy notice, please contact the School Business Manager.

Appendix 4 – Privacy notice Students, Parent and Carers

Privacy Notice for Students, Parents and Carers

Privacy Notice (How we use pupil information)

Why do we collect and use Student information?
We, Ruskin Community High School, collect and process Student information as part of our public function under both the Data Protection Act 1998 and General Data Protection Regulation. An example of this is the school Census return which is a statutory requirement on schools under Section 537A of the Education Act 1996. Ruskin High School is the 'data controller' for the purposes of data protection law.

We use the Student data:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections

The categories of student information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details, address and identification documents)
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- relevant medical information, including physical and mental health
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- student and curricular records
- details of any support received, including care packages, plans and support providers
- photographs
- biometric (thumb prints)
- CCTV images captured in school

We may also hold data about students that we have received from other organisations, including other schools, local authorities and the Department for Education.

Collecting Student information

Whilst the majority of Student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain Student information to us or if you have a choice in this.

Storing Student data

We hold personal information about students while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our Records Management Policy sets out how long we keep information about students.

How will my information be stored?

Ruskin High School uses an electronic database. The school also holds a Student file that is received from the Primary school.

Who do we share Student information with?

We routinely share Student information with:

- schools that the students attend after leaving us
- our Local Authority
- the Department for Education (DfE)
- NHS / School Nurse

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 information about our students with anyone without consent unless the law allows us to do so.

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. This data sharing underpins school funding and educational attainment policy and monitoring.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about students with:

- Our Local Authority – to meet our legal obligations, such as safeguarding concerns and exclusions
- The Department of Education - (a government department)
- The student's family and representatives
- Educators and examining bodies • Our regulator - (Ofsted)
- Suppliers and service providers – to enable them to provide the service we have contracted them for.
- Health authorities, Health and Social Welfare organisations
- Police forces, courts, tribunals
- Professional bodies

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 Students aged 13+?
Once our students reach the age of 13, we are legally required to 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 he/she reaches the age 16.

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.

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:
- 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 in compliance with the GDPR.

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
Will this information be used to take automated decisions about me? No

Will my data be transferred abroad and why?

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with Data Protection law.

Requesting access to your personal data
You have the right under the Data Protection Act 1998 (General Data Protection Regulation) to request a copy of your information and to know what it is used for and how it has been shared. This is called the right of subject access.

To make a request for your personal information, or be given access to your child's educational record, contact Student Services Manager, Ruskin Community High 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 H Goodwin, School Business Manager, Ruskin Community High School.