Data Protection Policy

Introduction

My Online Schooling aims to ensure that all personal data collected about staff, pupils, parents/carers, 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.

Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) (Amendment) Regulations 2018 which gives parents the right of access to their child's educational record.

This policy does not form part of a contract of employment; however, it is mandatory that all staff, partners or contractors must read, understand and comply with the content of this policy and must attend associated training relating to its content and operation.

Failure to adhere to this policy is likely to be regarded as a serious disciplinary matter and will be dealt with under My Online Schooling's disciplinary rules and procedures.

Definitions

Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and subsequently requires more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions

	• Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	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

My Online Schooling processes personal data relating to parents, pupils, staff and others, and is therefore a Data Controller.

My Online Schooling are registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles & Responsibilities

Data Protection Officer

- Data Protection Officer (DPO): Emily Leask, Head of Innovation
    - emily@myonlineschooling.com

The Data Protection Officer 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 are also the first point of contact for individuals whose data My Online Schooling processes and for the ICO.

This policy applies to all staff employed by My Online schooling and to external organisations or individuals working on behalf of My Online Schooling.

All staff are responsible for:

- collecting, storing and processing any personal data in accordance with this Policy
- informing My Online Schooling 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, or if they are unsure whether 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 UK or if there has been a data breach.
    - whenever they are engaging in a new activity that may affect the privacy rights ofindividuals.
    - 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 My Online Schooling must comply with. The principles say that personal data must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes.
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- accurate and where necessary, kept up to date.
- kept for no longer than is necessary for the purposes for which it is processed.
- processed in a way that ensures it is appropriately secure.

This policy sets out how My Online Schooling aims to comply with these principles.

Collecting Personal Data

Lawful, Fair and Transparent Processing

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

- the data needs to be processed so that My Online Schooling can fulfil a contract with the individual, or the individual has asked My Online Schooling to take specific steps before entering into a contract.
- the data needs to be processed so that My Online schooling 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 My Online Schooling 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 My Online Schooling 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 pupil) 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.

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

Privacy Notices

Before collecting or processing personal data directly from a data subject, My Online Schooling will ensure that an appropriate privacy notice has been issued to the data subject.

Different notices are used for employment and commercial purposes. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also explain how, when and for how long we propose to process the data subjects personal information.

My Online Schooling will include information around the data subjects' rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where My Online Schooling must collect data indirectly from a third party or a public source (i.e. electoral register), a privacy notice will be issued to the data subject within a reasonable of period of obtaining the personal data, no later than one month. If the data is used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

Data collected indirectly can only be used if there is sufficient evidence that it has been collected in accordance with the GDPR principles.

In all circumstances, only the up to date version of My Online Schooling's privacy notice should be used, and it can only be used in accordance with My Online Schooling's guidelines.

Limitation, Minimisation and Accuracy

My Online Schooling 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.

Kept Confidential and Secure

The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this, My Online Schooling will follow these steps:

- My Online Schooling has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
- Where My Online Schooling provides you with code words or passwords to be used before releasing personal information, for example by telephone, these must strictly follow My Online Schooling's requirements.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- Ensure that any personal data which is held is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another employee's records without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager.
- Ensure that when working on personal information as part of your job duties when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.

- Manual personnel files and data subject files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact the Head of Innovation. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets.
- Data held on computers are stored confidentially by means of password protection, encryption or coding.

Transferring Data to Another Country

Transfer of personal data to countries or organisations outside of the EEA should only take place if appropriate measures are in place to protect the security of that data.

We do not generally have a need to transfer data outside of the European Economic Area (EEA). However, if required to transfer personal data to a country or organisation outside of the EEA, My Online Schooling must not transfer personal data to a country or organisation unless that country or organisation ensures an adequate level of protection in relation to the processing of personal data and safeguards are in place to ensure this is done. Employees should consult with the DPO before transferring any data outside fo the EEA.

The Data Subject's Rights

The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that My Online Schooling should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights. Employees must follow My Online Schooling's policies and procedures whenever you process or receive a request in relation to any of the above rights.

Data Subject Request Procedure

Individuals have a right to make a subject access request to gain access to personal information that My Online Schooling 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.
- with whom the data has been or will be shared
- 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 should include the following:

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

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

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.

Junior School
Children below the age of 12 are generally not considered to be sufficiently mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Junior School, may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Secondary School
Children aged 12 and above are generally regarded as being sufficiently mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Secondary School may not be granted without the express permission of the pupil. This is not a rule and a pupil'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:

- will request the individual to provide two forms of identification.
- may contact the individual via telephone to confirm the request was made.
- will respond within one month of receipt of the request.
- will provide the information free of charge.
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

My Online Schooling 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 recognises 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 and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- withdraw their consent to processing at any time.
- 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 United Kingdom.
- 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.

Parental Requests to See the Educational Record

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.

Data Security and Storage of Records

My Online Schooling 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:

- portable electronic devices, such as laptops and hard drives that contain personal data are kept secure using appropriate password management, encryption, firewalls and lockdown procedures
- passwords that are at required to be changed on a regular basis are used to access school computers, laptops and other electronic devices.
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- 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 shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on My Online Schooling's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Categories of Information

My Online Schooling employees may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and in a confidential manner at all times. However, where that data is classed as a special category, extra care should be taken to ensure the privacy and security of that data. This means that employees should

maintain a high level of security and you should only share this data with those who are also authorised to process that data. In the context of employee relations the scenarios when you may be required to process special categories of information may arise for one or more of the following reasons:

- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting.
- And any other reasons which we advise you of under a separate policy or notice.

In order to comply with employment and other laws when processing and managing situations connected with absences arising in relation to sickness or family/dependant related leave.

To ensure health and safety obligations and other employment related obligations are met you may be required to process information about the physical or mental health or disability status of an employee in order to assess their capability to perform a role. Employees may also be required to monitor and manage sickness absence, recommend appropriate workplace adjustments and administer health related benefits.

My Online Schooling may also require employees to process special categories of information in connection with customers and other third parties.

There may also be circumstances where we ask employees to process this type of information in relation to assisting My Online Schooling with legal claims or to protect a data subjects interests (or someone else's).

Employees may be asked to process information in relation to criminal convictions. This should be processed with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

If you are unsure about how you should process general personal data or special categories of personal data, you must contact the DPO.

Exemptions

In limited circumstance there are certain categories of personal data which are exempt from the GDPR regime. In an employment for example:

- Confidential references that are given, but not those received by My Online Schooling from third parties. Only designated line managers can give references on behalf of My Online Schooling. Confidential references will not be provided unless My Online Schooling is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Personal Data Breaches

My Online Schooling 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 Annex A. 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:

- safeguarding information being made available to an unauthorised person.
- the theft of a My Online Schooling laptop containing non-encrypted personal data about a pupil.
- unauthorised users given access to a secure platform

Record keeping

As we have fewer than 250 employees, we only need to document processing activities that: are not occasional; or could result in a risk to the rights and freedoms of individuals; or involve the processing of special categories of data or criminal conviction and offence data.

Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or My Online Schooling processes make it necessary.

Sharing Personal Data

My Online Schooling will not normally share personal data with anyone else but may do so where:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- we need to liaise with other Agencies – we will seek consent as necessary before doing this.
- our suppliers or contractors need data to enable us to provide services to our staff and pupil, 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.

My Online Schooling 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.

My Online Schooling may also share personal data with emergency services and Local Authorities, to help them to respond to an emergency that affects any of our pupil or staff.

Direct Marketing

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints please in the first instance contact the Head of Innovation

Changes to this Policy

My Online Schooling reserves the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures.

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed on an annual basis.

Annex A

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 or altered.
    - Disclosed or made available where it should not have been to unauthorised people.
- The DPO will alert the Executive Headteacher
- 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 consider 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 or financial loss.
    - unauthorised reversal of pseudonymisation (for example, key-coding); damage to reputation or loss of confidentiality.
    - any other significant economic or social disadvantage to the individual(s) concerned
    - If it is 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 later challenged by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO.
- 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: o 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 or effects of 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 by the DPO.
- The DPO and Executive Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

My Online Schooling 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. My Online Schooling will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive Information Being Disclosed via Email *(including safeguarding records)*

- 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 take necessary measures 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.

Other types of breach could include

- a My Online Schooling laptop containing non-encrypted sensitive personal data being stolen or hacked.
- My Online Schooling's cashless payment provider being “hacked” and parents’ financial details stolen.

Annex B

Subject Access Request Form

General Data Protection Regulations Right of Access to Personal Data

We should respond to your request within one calendar month. Note this can be extended for a further two months if the request is deemed complex. However, this period does not start until:

- We are satisfied about your identity
- You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

Provide details of the person about whom My Online Schooling is holding the data (Data Subject)	
Full Name:	
Date of Birth:	
Present Address:	
Previous Address: *(if less than 3 years at your present address)*	
Telephone Number:	
Email Address:	

Are you requesting information about yourself? If **YES**, skip this section. If **NO**, please complete the following.	
Full Name:	
Present Address:	
Telephone Number:	
Email Address:	
Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:	
If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject	

Please provide a clear description of the information that you are requesting, see table below. If you provide specific details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.

Description of Information	Time Period for Information Requested

Please provide two original documents as evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity include

- Driving Licence
- Passport
- National ID Card
- Medical Card
- Utility Bill

Your documents will be verified on a Zoom call with the Data Protection Officer.

All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information.

Declaration

To be completed by all applicants. Please note that any attempt to mislead My Online Schooling may lead to prosecution.

I (insert name)

certify that the information given on this application form and any attachments therein to My Online Schooling is accurate and true. I understand that it is necessary for My Online Schooling to confirm my identity and it may be necessary to obtain more information, in order to locate the requested information.

Signature:	
Date:	

Return of the Form

If you are posting your request thn our address is detailed below:

For the Attention of the Data Protection Officer
84 Commercial Street
% My Online Schooling
Edinburgh, EH6 6LX

Our email address is emily@myonlineschooling.com

How we will send you the information you have requested

We want you to receive the information you have requested in the most convenient way for you. However, we do have an obligation under the General Data Protection Regulations to provide you with the information you have requested in the most secure way possible.

We believe the most secure way to provide you with the information is for us to email you the information securely/encrypted.

We can post your information to you but there are risks attached to providing you with your information using this method, eg your information may be lost by the delivery service or delivered to the wrong address.

Please confirm you are happy to receive your information by secure email by ticking the box below and confirming the email address that your information should be sent to:

Confirmation:		Email Address:	

Alternatively, if you prefer any of the other methods below please indicate which by ticking the box below:

By Post:		CD or Paper Copy *(please circle or highlight your choice)*