ICO Registration Number: ZA048541
Expires: 22nd April 2024

Scope:

The Write Time Data Protection Policy is an organisation-wide document that is directly applicable to all staff, consultants, volunteers, and any stakeholder that has access to any data within the control of The Write Time.

Introduction
The Write Time is committed to protecting the rights of individuals to privacy concerning the collection, processing and storage of personal data. To achieve this aim, The Write Time must ensure that robust safeguards are in place within the organisation to prevent unauthorised disclosure, access, duplication, publication, loss, alteration, manipulation, theft, or deletion of data within its control.

This document together with the documents that form the Information Security Management System[1] (ISMS) is the process which will protect the data within the control of The Write Time.

Data Protection is governed by statute Law. The Data Protection Act 2018 provides principles with which The Write Time must comply to legally protect all data within its possession.

In summary, these principles state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for that purpose
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose
- Be processed under the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data

[1] All policies related to data and IT/ICT

These eight underlying legal requirements are the basis for the policies, procedures and processes that The Write Time has put in place to protect personal data (information). As stated in the scope of this policy, any person that has access to The Write Time controlled data must ensure that they always follow organisational procedures and processes which encompass these principles.

Status of this Policy

This policy does not form part of a contract of employment, but it is a condition of employment or access to provision/services employment or part of a learning agreement for learners/clients delivered by The Write Time that this policy and its requirements are followed and incorporated into any duties performed on behalf of The Write Time. Any failures to follow the agreed, policy, procedure and processes will result in disciplinary proceedings for employees or alternate legal redress for other business relationships.

Under the provision of the 2018 Act, The Write Time must register with the Information Commissioner's Office (ICO) (**Registration number:** ZA048541**)** stating the range of the organisation's activities and the purpose for which data will be collected.

The Write Time must also name a Data Controller and register this individual with the Information Commissioner Office (ICO). Chris Murray (Managing Director) is the designated Data Controller for The Write Time and is therefore ultimately responsible for policy implementation.

The Designated Data Controllers are:

For Employees:

School Office Manager: Amirah Khaldi

For The Write Time to operate as an organisation it needs to obtain and process certain information about its employees, students, customers and additional stakeholders to allow the organisation to fulfil its daily operations and to meet any statutory requirements and obligations, e.g., the payment of taxation, any inspection requirements and obligations for Ofsted etc. To comply with the law, information collected must be used fairly, stored safely and must not be unlawfully disclosed to any unauthorised person.

Responsibilities of Staff
All staff are responsible for:

- Verifying that any employee information held by The Write Time is accurate and up to date
- Updating The Write Time with any changes to their personal data such as change of address, be it at the time of appointment or subsequently

The Write Time cannot be held responsible for any errors unless the staff member has informed The Write Time of such changes.

When, as part of their responsibilities, an employee collects information about an individual (e.g., about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with all policies and procedures.
All employees that as part of their role must collect, process and store personal data of a learner/customer of an additional stakeholder must ensure that all personal data provided to The Write Time is accurate and up to date.

Data in transit
The working definition of "data in transit" for this policy has been written to be plain and as uncomplicated as possible to understand. For this policy, 'data in transit' is to be defined as **when data is in the process of being moved from one place to another.**

Data can be in transit in 2 main ways, either physically in the real world i.e., the moving of actual paper documents from one place to another by hand, car, bus, train taxi, courier or by mail etc. Alternatively, data in transit can occur electronically in the digital world too, i.e., the use of email, fax, FTP (File Transfer Protocol) upload, portable storage media, and exchange of media format. Also, note that format change will also include the printing of a document.

This section of the policy is intended to prevent the accidental loss, or disclosure of data while on the move i.e., in transit.

If data is to be moved by an individual it must be appropriately protected during the moving/transit process and it is the responsibility of the individual performing the transit to assure this occurs.

"Appropriate" is not defined in terms of hard and fast rules, but is, in practice, a proportionate degree of security precautions specifically applied to the sensitivity of the data in transit and the potential impact of accidental loss or disclosure.

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data must assume personal responsibility and make considered judgements in terms of how they handle the data in their care whilst moving it.

When determining the specific precautions to take for the moving of data the overall impact of the potential loss or disclosure of the data is to be judged by assessing four areas of concern.

- The degree of sensitivity of the content of the data, i.e., whether personal or commercial (see appendix 1)
- The quantity of data, whether transferring a single record or a group of records
- The route/distance the data is going to take, and the method used for the transfer, i.e., which form of transit, by foot, car taxi etc.
- Any data that is to be transferred in whatever medium, if the security classification of the content is "**Restricted**" or higher (see appendix 1 for definitions) all transfers must be recorded on a log (see appendix 2 for a copy of the transit log)

It is essential to remember that while the amount of data being transferred is a logistical factor, the potential consequence of loss of a single record can be as damaging as losing 10 or 100 records to that one individual.

If in any doubt, any staff member that needs to transfer data can seek support from Amirah Khaldi, a named data controller or their line manager.

Key points:

- All The Write Time employees will be held personally responsible for any data which they have in their possession for the purposes of data in transit as defined above

- An appropriate transfer bag/container for the transport of data will be provided for each centre when required. All staff required to transfer data will be required to use this specifically provided a fit-for-purpose medium for transport. If the data needing to be transported will not fit into the transfer bag or it is not available, then a fit for purpose and suitable alternative must be agreed with their line manager to ensure the protection of the data during transport[2]

[2] Note a line manager can always seek advice from a data controller or a member of SLT before authorising the transfer

- Only The Write Time employees or contacted consultants may transfer any The Write Time data / material.
- Individuals need to ensure that if data is to be taken out of the protected environment of the office / server it is suitably protected in proportion to the consequences of loss or disclosure of the content material, i.e. the more sensitive the data the more precautions are to be taken.
- If data/materials are to be transferred by an employee's car[3], no data/documents are to be left in an unoccupied car, especially if it is needed to be stored overnight.
- Any data which is considered "Restricted" and above and is stored in electronic format, must be encrypted if it is taken outside of its normally secure location
- Any Data loss must be reported immediately to your line manager, and a member of Senior Management must also be informed
- All employees are reminded that they must be fully aware of The Write Time's Data Protection Policies and procedures before handling sensitive or confidential personal data
- Ensure that if the data being transferred is classified "Restricted" or above the appropriate log must be completed
- Disciplinary action will be taken where The Write Time employees do not follow the guidance set out in this Policy

All employees are responsible for ensuring that:

- Any data in whatever format it is collected or gathered (electronically or on paper) is kept securely according to its protective marked status.
- Personal data is not disclosed either orally, in writing, via Email or Web pages or by any other means, accidentally or otherwise, without the consent of the data owner.

[3] Note: The use of own car for company use will require your car insurance to cover business use.

Employees should note that deliberate or negligent unauthorised disclosure will be a disciplinary matter and may be considered gross misconduct in some cases.

Any data which is considered Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe
- If the data is computerised, it is to be a minimum of password protected and stored on the network server, which is protected and regularly backed up
- **NB. Storage of (customer) personal data is not permitted on local storage (i.e., C drives on PCs or Laptops)**
- Any data that has a protection mark of restricted and above cannot be copied on any form of removable storage media, without the Privilege right granted by the School Office Manager, Amirah Khaldi. Once copied the media must itself be kept in a locked filing cabinet, drawer, or safe
- Where the organisation has dictated that data attributable to a named project or programme is to be afforded additional protection above that of normal data, all local or specific policies, procedures and processes must be always followed.

Disclosure

There are certain circumstances when The Write Time may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. This will only be completed with the informed consent form of the individual.

There are circumstances where the law allows The Write Time to disclose data (including sensitive data) without the data subject's consent[4]. These are:

[4] During their inquiries, the police may wish to obtain personal details regarding an individual that relates to an alleged offence, or information about a range of individuals or members of staff that fit a suspect. Although the police have no automatic right to such information, The Write Time will want to be seen as assisting the police with any enquiries and as such will consider the use of S29 the Data Protection Act. Under the Data Protection, Act 2018 the sharing of information is permissible for the Prevention & Detection of Crime without the consent of the individual to whom the information refers. This is also known as a Section 29 disclosure. However, the use of section 29 allows data to be released for this purpose without the consent of the owner, but it does not override other principles or duties of the act.
If you receive a request for disclosure of the information you need to consider the following.

- What is the alleged crime and what is the seriousness of the alleged offence? Sometimes it can be quite obvious i.e. Murder and at other times, less so, for example, petty theft.
- Ask them to justify why they need the information, and do they need the amount of information they are requesting

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of an Individual/Service User or another person

c) The Individual/Service User has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e., race, disability or religion

f) Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g., where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures

The Write Time regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Rights to Access Information (Subject Access Request)

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this and an individual who makes a written request and pays a fee is entitled to be:

- Who is making this request for information? Are they of sufficient seniority within their own organisation to accept responsibility for that organisation? Remember, it is a criminal offence to knowingly or recklessly obtain or disclose information without the consent of the organisation.
- Always ask for a request formally, in writing and on the organisation's headed stationery.

Remember that just because the police may quote Section 29 of the Data Protection Act does not mean that we are obliged to comply with that request. If you have genuine concerns about releasing the personal information (for example, because you think you have other legal obligations such as the information being confidential), then you can ask the police to come back with a court order requiring the release of the personal information. If the court decides you should release the information, you will not break the Act by obeying the order.

Any such requests must be referred to one of The Write Time's Data Controllers (See Data Protection Policy) who will consider the validity of the request. The Data controllers will make a recommendation as to whether to agree to the request or refuse the request it may be necessary for a Member of SLT or The Write Time legal representation to authorise the release of the information.

- Told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the information comprising the data; and
- Given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions, or an assessment of performance at work (except where this information is a trade secret).

The Write Time will make a nominal charge of £10 Administration charge on each occasion that access is requested, although The Write Time has the discretion to waive this.

The Write Time aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the time frames required by the 2018 Act.

Examination Marks

During the course of their studies, students will routinely be provided with information about their marks for both coursework and examinations (if applicable). However, exam scripts and online test answers are exempted from the subject access rules and copies will not ordinarily be given to a student who makes a subject access request.

Subject Consent

It is best practice that The Write Time can only collect and process personal data with the informed consent of the individual. If the individual is a young person (defined as a person aged between 13 to 19) best practice dictates that a young person aged 16 and over can give informed consent, for young persons below 16 a judgment must be made about their ability to understand what is being asked of them. They should have clear and intelligible information about the request for information suited to their level of understanding. All young people under the age of 16 will be encouraged to involve their parent/carer to also provide consent, but where a request is specifically made not to involve a parent an informed consent of a minor has to be approved by a member of SLT.

The Write Time respects that individuals have a right to privacy and have the option to refuse to provide consent for the collection or the sharing of personal data as it is their choice. However, this right to refuse must be balanced with The Write Time's need to evidence their activities. If a potential customer or an existing customer exercises their right to refuse consent to collect or share personal data, this may result in The Write Time's ability to allow access to a service or provision delivered by The Write Time.

Some employment roles (or courses) will bring the applicants into contact with children, including young people between the ages of 16 and 18. The Write Time has a duty under the Children Act 2004 and other enactments to ensure that employees are suitable for the job role, and have access to young people.
The Write Time also has a duty of care to all employees, learners/clients or additional stakeholders and must therefore ensure employees and those using The Write Time facilities do not pose a threat or danger to other users.

The Write Time may also ask for information about health needs, such as allergies to forms of medication, or any medical condition such as asthma or diabetes. The Write Time will only use this information for the protection of the health and safety of the individual but will need informed consent to process this data in the event of a medical emergency.

Therefore, any application form that a prospective employee applying for a job at The Write Time or prospective learner is required to complete will include a section requiring consent to process the applicant's personal data. A refusal or failure to sign such a form will prevent the application from being processed.

NB. This includes information about non-spent previous criminal convictions and in certain employment conditions information about spent previous criminal convictions.

Processing Sensitive Information

Sometimes it is necessary to process information about an individual's health, criminal convictions, race, and trade union membership. This may be to ensure that The Write Time is a safe place for everyone or to operate other The Write Time policies, such as the sick pay policy or the equality & diversity policy. Because this information is considered sensitive under the 2018 Act, staff (and students where appropriate) will be asked to give their express / informed consent for The Write Time to process this data.

NB. An offer of employment or access to a service or provision delivered by The Write Time may be withdrawn if an individual refuses to consent to this without good reason.

Publication of The Write Time Information

Certain items of information relating to The Write Time staff will be made available via searchable directories on an internal intranet system, to meet the legitimate needs of fellow employees, Inspectors or other legitimate visitors.

The Write Time may request (seek informed consent) to make additional employee, student/client or additional stakeholder biographical details or other personal data available e.g., academic or vocational successes made on their public websites for promotional activities. Examples of this form of request would be to publish a student's success story, produce a case history or publish a photograph. In most cases, anonymous case histories will be used which will not require consent.

Retention of Data

The Write Time must retain some employee, learner/client personal data for some time following their departure from The Write Time, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, to evidence funding requirements have been met for example relating to pensions and taxation. Different categories of data will be retained for different periods. The exact details of retention periods and purposes are set out in the Data Retention Policy.

Conclusion

Compliance with the 2018 Act is the responsibility of all members of The Write Time. Any deliberate breach of the data protection policy may lead to disciplinary action being taken or access to The Write Time's facilities being withdrawn, or even criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the appropriate Designated Data Controller (Chris Murray).

Appendix 1:

The Write Time classifies information into four levels of classification (confidential, restricted, protected and unclassified).

Confidential:
This classification applies to information that is an access restricted specifically to the Directors and SLT and specifically named professional advisers authorised by either one of these two levels.

Information that falls into this category must be marked 'Confidential', and its circulation is kept to a minimum with the names of the people to whom it is limited identified on a master list held by the executive assistant to the chief executive.

If a document classified as confidential is needed to be copied, the number of copies produced must be recorded on a central register, this register is retained for tracking and identifying the recipient of each copy.

Examples of confidential information might include information about potential acquisitions or corporate strategy, or about key organisational personnel, such as the Managing Director (MD).

Confidential information can only be sent by encrypted email and a digitally signed secure email carrier service, in line with Section 12.3 of the ISMS, and sent only to the e-mail box of the identified recipient. Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine. The amount of information that falls into this category should be carefully limited; the cost and operational inconvenience of protecting it properly are such that it needs only to be information whose release can significantly damage the reputation or financial security organisation.

Restricted (Restricted + Sensitive)
Restricted information of this category is an access restricted to specific named employees working in a role where access to this level of data is required to perform their respective duties for the organisation. Emails that need to contain restricted information will need to be a minimum of password protected.

This classification encompasses all types of personal information for employees and or clients/customers. All information assets have value, but personal details are required to be specifically protected by law (Data Protection Act) Examples would include the following: Name, Address, Telephone / Mobile numbers, Email address, Age, Gender, Ethnicity, Work History, and National Insurance Number (NINO).

Restricted + "Sensitive" This is a special subset of the restricted category that is applied to 8 specifically identified pieces of personal information in the Data Protection Act. Whereby disclosure of these specific details has the potential to cause additional harm than other standard personal details, and sensitive data if

collected, is subject to a higher standard of care, i.e., Afforded greater protection, Restricted + "Sensitive" information cannot be emailed unless the content is encrypted.

(a) The racial or ethnic origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Whether is a member of a trade union (within the meaning of the M1 Trade Union and Labour relations [consolidation] act 1992)

(e) Physical or mental health or condition

(f) Sexual life

(g) The commission or alleged commission by him of any offence

(h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

In addition to these 8 named details identified in the Data Protection Act, as a matter of best practice, The Write Time is adding a category of data to this subset: Any details connected with an individual's financial records (if collected) will be considered sensitive data and afforded greater protection (e.g. salary, tax returns, bank account details).

Protected
This classification covers information assets that have a commercial value, but which do not need to fall within either of the higher categories. This level of classification includes commercial and sensitive commercial information which may be advantageous to a competitor, examples include partnership agreements, details of funder payment values and cost. This level of classification may also include contract delivery plans.

Any member of staff employed by The Write Time is entitled to access information with this classification, by nature of their employment if there is an operational business need for the data to be accessed.

This classification of information is not cleared for release outside the organisation and is subject to the protection of the organisational confidentiality and data protection policies. As such if any protected information needs to be sent by email it must be password protected (See: Password policy) secure email need not be used.
Information and documents that would be considered protected could include, organisation expenses details, utility costs for the delivery centres, invoices and bills (Utility) as these documents could contain information that the organisation would not necessarily want the general public to know of.

Most of the internal use only documents, memos, emails and policy formulation will be considered protected.

Unclassified
Any asset or document that is security marked as unclassified is to be considered as being within the public domain. Any unclassified document can be released or distributed outside the organisation. An example is that all The Write Time Policies and Procedures are to be considered as unclassified (but are only to be provided on request and are to be provided in a suitable for purpose format.)

There are no restrictions on the transport or transfer of unclassified assets.

Log of Information Assets for Transfer Form

Date of transfer	Item description	State the classification level of the material	Manner of transport	Details of transfer (from and to locations)	Number of items in transfer	Authorising Manager	Declaration from employee that data is transit secure (signature)	Date Signed in new location