THE GEMS LEARNING TRUST DATA PROTECTION POLICY

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection
- Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following other trust policies:

- E-safety Policy
- Freedom of Information Policy

Definitions

Data subject	The individual in relation to which the academy is holding information about; in our context this is parents, pupils, staff, agency workers, governors and trustees.
Personal data	Information relating to identifiable individuals, such as parents, children, relatives, job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. Personal data we gather may include: individuals' contact details, addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

	Personal data may be collected from parents, staff, other schools, children, LAs, and the Department for Education.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data is strictly controlled in accordance with this policy.

Scope

This policy applies to all staff, parents and children. Academy staff must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to staff use of internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Our Data Protection Officer, Beth Gorsuch has overall responsibility for the day-to-day implementation of this policy.

Data Protection Officer

Each organisation must appoint a DPO. They can be an employee or the role can be contracted out. They must report to the highest level of management in the organisation, eg the Board. They must have adequate resources to meet their GDPR obligations.

The Data Protection Officer's responsibilities:

- Inform and advise the organisation and employees about duties and obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed
- Keep the board updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from parents/carers, staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by the GEMS Academies
- Ensuring third parties that handle the company's data any contracts or agreement regarding data processing are compliant with the GDPR. Third parties must comply with 11 clauses of the GDPR
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

- Ensure all IT systems, services, software and equipment meet acceptable security standards
- Ensure checking and scanning security hardware and software is carried out regularly to ensure it is functioning properly
- Researching third-party service providers, such as cloud services the company is considering using to store or process data

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The processing of all data must be:

- Necessary to provide our educational environment
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine data processing activities.

Justification for personal data

We will process personal data in compliance with all eight data protection principles:

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

We document any additional justification for the processing of sensitive data.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one

purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, Beth Gorsuch.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Consent and conditions for processing data

Some data that we collect is subject to active consent by the data subject. This consent can be revoked at any time. Some data we collect is in relation to our legal responsibilities as set out in article 6 of the GDPR:

6(1)(a) Consent of the data subject

6(1)(b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) Processing is necessary for compliance with a legal obligation*

6(1)(d) Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) 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

6(1) (f) Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

*Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. Privacy notices for staff, parents and pupils can be found on each academy and Trust website.

The notice:

- Sets out the purposes for which we hold personal data on parents, children and employees
- Highlights that our work may require us to give information to third parties
- Provides that our stakeholders have a right of access to the personal data that we hold about them

Personal data

Individuals and data subjects must take reasonable steps to ensure that personal data we hold about is accurate and updated as required. For example, if personal circumstances change, please inform the relevant academy so that they can update your records.

Sharing personal data

It is necessary to share personal data with third party organisations. It is our responsibility to ensure that the data we share is compliant with the conditions of processing and is shared in a secure manner.

Third parties include:

- HR providers
- Payroll providers
- Social Services
- Recruitment agencies
- Banks
- Pension providers – TPS, LGPS, other
- Local Authorities
- Department for Education
- ESFA
- External accountants
- Occupational health providers

We abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

We do not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Sensitive data will be shared on a needs basis with appropriate access controls.

Sensitive data will be collected on the following grounds

- Explicit consent has been given

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment… law.

- Processing is necessary for the reasons of substantial public interest, on the basis of Union or Member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Privacy by Design and Privacy Impact Assessments

The trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the trust has considered and integrated data protection into processing activities. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the trust's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to GEMS Learning Trust's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

DBS checks and personal data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

CCTV

Academies must display a sign showing the use of CCTV cameras for the purposes of safety and security. Data should be stored for limited periods of time. Cameras should not be placed in areas where privacy can be breached.

Academies must register use of their CCTV with the ICO ico.org.uk/registration/new

The Principal, Office Manager, Premises Manager and DPO have access to CCTV images.

Each academy must have a CCTV policy.

Photography

The trust/academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the trust wishes to use images/video footage of pupils in a publication, such as the trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

Data security

We keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for ensuring that all data security processes and IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Storing data securely

- In cases when data is stored on printed paper, it is kept in a secure place where unauthorised personnel cannot access it
- Printed data is shredded when it is no longer needed – use data deletion processes as set out in this policy
- Use secure remote access software for accessing school systems from another location
- Ensure each academy has an Access Control list – defining who has access to data, systems and administrator access is limited to just a few users
- Ensure network permissions are set correctly so users can only access the data and files they require to carry out their duties
- All network users have individual logins. Don't share usernames or passwords.
- Passwords must be adequately complex and changed periodically.
- We encourage all staff to use a password manager to create and store their passwords.
- Devices such as laptops, tablets and mobile phones should be locked away when not in use.
- Ensure antivirus and malware software are up to date as well as operating systems on laptops, tablets and mobile phones
- Mobile phones are password protected and able to have their content accessed/deleted remotely

- Screen locks should be in place for users of MIS systems and other software packages containing personal data
- Emails containing personal data should not be sent from staff/governor/trustee personal accounts.
- Staff should be vigilant of emails with suspicious attachments, from emails addresses who have similar name configurations hyperlinks and proceed cautiously
- Ensure staff complete basic 'cyber security' training in relation to opening emails, scanning USBs, handling personal data etc
- Ensure wireless network is password protected and encrypted
- Data stored on CDs or memory sticks is encrypted and locked away securely when not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data are kept in a secure location or in the cloud, away from general office space
- Data is regularly backed up in line with the company's backup procedures
- Data is never saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data are approved and protected by security software and a strong firewall.
- Staff must report loss of a device; laptop, mobile phone, tablet etc immediately to the Principal
- Keep a record of third party access to data – eg payroll companies, pension providers etc.

Data retention periods

We retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.

Documents will be stored in line with guidance stated in the document retention schedule set out by the IRMS.

Data deletion

Disposal of records that have reached the end of the minimum retention period **should be deleted or archived in line with the following guidance in relation to the principle of the GDPR that** personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purpose.

In each **academy**, **office/business** managers must ensure that records that are no longer required are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the records management policy within the organisation.

Safe destruction of records
All records containing personal information, or sensitive policy information should be made either unreadable or un-reconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The academy must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by the Principal and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

Freedom of Information Act 2000 (FoIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction

Office/Business managers should record at least:

• File reference (or other unique identifier);

• File title (or brief description);

• Number of files and date range

• The name of the authorising Principal

• Date action taken

Transfer of records to Archives

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service. The school should contact

the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the GDPR and the FoIA 2000.

If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British

Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Recording of all archiving, permanent destruction and digitisation of records

Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

Transferring data internationally

There are restrictions on international transfers of personal data. No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA. Any transfer personal data anywhere outside the UK must be approved by the Data Protection Officer

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. **No charges** should be made to the data subject. Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within **one month**, provided there is no undue

burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

The Trust/Academy has one month to provide a full response to the data subject. Data subjects can be encouraged to submit requests during term time but are under no legal obligation to do so.

If you would like to make a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests. There are also restrictions on the information to which you are entitled under applicable law.

Right to be forgotten and to Rectification

A data subject may request that any information held on them is rectified, deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the trust will inform them of the rectification where possible. Where appropriate, the trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, the trust will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to restrict processing

Individuals have the right to block or suppress the trust's processing of personal data. In the event that processing is restricted, the trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the trust has verified the accuracy of the data
- Where an individual has objected to the processing and the trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The trust will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The trust will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. GEMS Learning Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the trust will consider whether providing the information would prejudice the rights of any other individual. The trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an objection is received.

• The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

• The individual must have grounds relating to their particular situation in order to exercise their right to object.
• Where the processing of personal data is necessary for the performance of a public interest task, the trust is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the trust will offer a method for individuals to object online.

Staff contracts/HR

DPA clauses in staff contracts are no longer legally compliant with the GDPR. Letters of variation will be issued to existing staff and all new staff will be issued with GDPR compliant data protection processes.

Information given in staff references must comply with the GDPR.

All HR policies must be reviewed to ensure they are GDPR compliant, including the staff handbook.

Staff references

Training

All staff receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house session on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

Data breaches

Staff should notify the Principal or the DPO **immediately** if they are concerned about a possible data breach.

If a breach is discovered outside of term time by a staff member, they should alert the DPO immediately.

Reporting breaches

Data breaches must be reported to the ICO within 72 hours. If the breach is sufficiently serious to warrant notification to the public, the breach must be reported without undue delay.

If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Checklist for data breaches

1. Mobilise a crisis management team – Principal, Office/Business Manager and DPO
2. Assess level of risk of data breach – no risk/risk/high risk – if unaddressed such as breach is likely to have a significant detrimental effect on individuals /data subjects
3. Inform the ICO within 72 hours
4. DPO to keep records of response to the data breach
5. Identify key internal and external messaging for communications strategy and issue
6. Secure IT systems
7. Stop additional data loss
8. Speak to those affected/involved: If there is a high risk to the rights and freedoms of individuals, data subjects must be notified.
9. Identify key issues and extent of data breach
10. Review protocols about disseminating information about the breach for everyone involved
11. Begin an in-depth investigation, using forensics if necessary
12. Report to police when/if considered appropriate
13. Notify regulators/consult with legal team/insurers/RPA etc

What information must a breach notification contain?

1. The nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
2. The name and contact details of the data protection officer
3. A description of the likely consequences of the personal data breach; and
4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both the staff and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Contact:

If you would like to discuss anything in this privacy notice, please contact:

- Beth Gorsuch, Data Protection Officer gemslearningtrust@gemseducation.org