Information Governance Policy

Including, Data Protection, Information Security, Freedom of Information, Records Management and Subject Access Requests

Contents

1. Information Governance Policy

This document is a statement of the aims and principles of the Enquire Learning Trust (the Trust) for ensuring the management of information.

The Information Governance Policy (IGP) addresses the following areas:

- Governance and Compliance – i.e. the actions the Trust and its Academies will undertake to ensure compliance with the IGP.
- Data Protection Policy – i.e. the confidentiality, integrity and availability of personal data and sensitive personal data relating to governors, employees, pupils, and parents / carers.
- Induction – i.e. information about the process to follow to induct all new employees into the Enquire Learning Trust
- Information Security Policy – i.e. the technical and organisational measures to be adopted by the Trust to manage the security of information.
- Freedom of Information Policy – i.e. managing public access to information created and held by the Trust.
- Records Management Statement – i.e. to the extent that the issues are not addressed by 1.2-1.4, the IGP also addresses records management (e.g. record retention and disposal; record keeping).

The following policies involve the collection and use of information, but are separate policy areas covered by their own separate policies:

- Safeguarding
- Online Safety
- Preventing Radicalisation
- Finance
- Procurement Policy
- Induction Policy
- Home Working
- Social Media

Version History

Date	Author	Version	Comment
25th October 2016	Gary Shipsey, Protecture	1.0	Drafted first version
8th February 2017	Gary Shipsey, Protecture, Brett Webster and Liz Thompson, ELT	2.0	Final draft for Trustees
7th July 2017	Gary Shipsey, Protecture, Brett Webster and Liz Thompson, ELT	3.0	Current version
9th April 2018	Brett Webster, Lauren Stones	4.0	GDPR Compliant
23rd July 2018	Brett Webster, Lauren Stones	5.0	Annual Trust Policy Review
1st January 2019	Brett Webster, Lauren Stones	6.0	ICO Recommendations

Governance and Compliance

In accordance with the Scheme of Delegation, the following governance arrangements and accountabilities will be in place with regards the IGP:

Board of Trustees (Level 1)

- The Board of Trustees will agree the IGP and related policies and are ultimately accountable for compliance across the Trust and its Academies.

Trust Directors – i.e. central support team

- The Trust Directors will allocate a role to be responsible for leading on compliance with the IGP across the Trust and its Academies.
    - This role should have sufficient understanding, or otherwise be able to access such understanding, of the information governance legislation that affects the IGP.
    - This role will be the named point of contact with the Information Commissioner's Office (ICO) and for any queries about the IGP made by employees and/or the public.
    - The Data Protection Officer (DPO) will be allocated this role.
    - The Director of Information Technology will be responsible for ensuring technological measures are put in place in each academy and the Trust centrally.

Information Governance Strategy Group

The IG Strategy Group consists of; Liz Thompson (DPO), Paul Kennedy (Deputy DPO), Lauren Stones (HR), Brett Webster (IT), Lynsey Freear (Responsible Officer) and Richard Hildyard (Trustee responsible for Information Governance)

Academy Principal (Level 3)

- The Principal, Vice Principal or Business Manager of an Academy will be accountable for compliance with the IGP for their Academy.
    - The Principal or Vice Principal may delegate day-to-day activity to their Business Manager.
    - The Principal, Vice Principal or Business Manager will report on their Academy's compliance with the IGP to the Trust Directors as required by the Board of Trustees.

Data Champions & All employees

- Data Champions in each academy have been identified and appropriately trained and will be the first point of contact for all employees.
- The Trust and all employees or others who process or use information which is the responsibility of the Trust must adhere to the IGP and related policies and guidance at all times.

Status of this policy

- The IGP does not form part of the contract of employment for employees, but it is a condition of employment that employees will abide by the rules and policies made by the Trust and academies. Any failures to follow the IGP and the related policies and procedures can therefore result in disciplinary proceedings, in accordance with the Discipline Policy.
- Breaches of the Information Governance Policy may be deemed to constitute gross misconduct dependent on the severity of the breach, and breaches may therefore result in dismissal.

Notifications under the General Data Protection Regulation and Freedom of Information Act 2000

- The Trust as a body corporate is registered as a Data Controller with the Information Commissioners Office (ICO). Academies that are members of the Trust are also named in the registration as joint Data Controllers.
- As such, the Trust shall maintain one notification for the Trust and Academies. The registration number is: ZA004552. Annual renewal date: 11 September
- The Notification shall be reviewed annual by the DPO and updated whenever a new Academy joins the Trust.

2. Data Protection Policy

The Enquire Learning Trust and its academies need to keep personal data about its employees, pupils and other users to allow it to monitor performance, achievements, health and safety, to process data so that employees can be safely recruited and paid, to manage the professional development of employees and to discharge other functions associated with the provision of education. In addition, there may be legal requirement to collect and process personal data to ensure that the Trust and its academies comply with statutory obligations.

The Enquire Learning Trust is the Data Controller.

The Trust is committed to ensuring the appropriate use and management of personal information at all times. The Trust and its academies will therefore adhere to the following guiding principles and detailed requirements:

- Transparency: inform individuals why the information is being collected; when their information is shared, and why and with whom it was shared.
- Rights: right to object, to erasure, for data processing.
- Quality: check the quality and the accuracy of the information it holds; not retain it for longer than is necessary, and ensure that when obsolete, information is destroyed appropriately and securely.
- Security: ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Sharing: share information with others only when it is legally appropriate to do so.
- Subject Access Requests and other disclosures: set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Training and Awareness: ensure our employees are aware of and understand our policies and procedures.
- Reporting of Actual or Suspected Breaches: ensure the Trust is aware of an actual or suspected breaches of the IGP, in order for it to be able to quickly assess the situation and take actions to reduce any risks.
- The identification and appointment to the role of the Data Protection Officer.

Transparency

Fair collection – general statement

The Trust and its Academies will only process personal data where;

- The consent of the individual has been obtained;
- Where the processing is necessary to comply with its legal and/or contractual obligations;
- It is necessary for the protection of someone's vital interests, or
- It is necessary for the Trusts legitimate interests or the legitimate interests of others.

The Trust and its Academies will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life,

criminal proceedings or convictions, where a further condition is also met. Usually this will mean that the individual has provided explicit consent, or that the processing is legally required for employment purposes.

Fair collection – Privacy statements

The Trust and its Academies will publish Privacy Notices on the Trust and academy websites – see Appendix 1, to provide any further information deemed necessary to ensure individuals are informed about the collection and use of their personal information. This must include details of how individuals can complain about possible any non-compliance with this policy or the data protection act, and provide a named contact.

Termly DPO audits will monitor the compliance of these Privacy Notices and provide recommendations for any changes will be reported to the Information Governance Strategy Group.

Fair collection – Multi-purpose parental consent

The Trust and its Academies will use a consent form to collect and record individual consent and parental / Guidance consent for the use of data for any Academy purpose – see Appendix 2.

Consent when obtained will be recorded into SIMS and this used for audit purposes to review and monitor consent given, and information held.

Monitoring

The Trust will monitor use of networks and systems to observe compliance with its policies. This is done irrespective of whether your use a Trust owned or personal device, to access or use, Trust information, network or systems. More details on the Trusts monitoring policy can be found within the Employee Privacy Statement – Appendix 11.

Systems that will be monitored by the Trust are:

- Content Filter – All Internet activity
- Futures Cloud – All computer activity
- Email – All email activity

Use of employee information

The Trust and its Academies will process data about employees for legal, personnel, administrative and management purposes in order to enable it to meet its legal obligations

as an employer, for example to compensate employees, monitor performance and to confer benefits in connection with employment.

The Trust and its Academies may process sensitive personal data relating to employees as specified within the Trust's Employees Privacy Statement – Appendix 11.

Rights

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Quality

Adequate, relevant and non-excessive processing

Personal data will only be processed to the extent that it is necessary for the Trust and/or Academy's specific purposes.

Accurate data

The Trust and its Academies will undertake reasonable measures to maintain the accuracy of personal information it processes.

- The Trust and its Academies will invite individuals to inform them if their personal details change or if they become aware of any inaccuracies in the personal data held about them.
- All employees are responsible for checking that any information that they provide to the academy in connection with their employment is accurate and up to date, and for informing the academy of any changes to information that they have provided (e.g. change of address) either at the time of appointment or subsequently – the academy cannot be held responsible for any errors unless the employee has informed the academy of such changes.
- All employees are responsible for maintaining accurate records about other people – e.g. about a pupil's homework, opinions about ability, references to other academic institutions, or details of personal circumstances – they must follow the Trust's "Accurate Record Keeping Guidance" where applicable – see Appendix 3

Data retention

The Trust and its Academies have a duty to retain some employees and student personal data for a period of time following their departure from the academy, mainly for legal

reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

The Trust and its Academies will not keep your personal data for longer than is necessary for the purpose it was originally collected for. This means that data will be destroyed or erased from our systems when it is no longer required.

The Trust and its Academies will adopt and adhere to the Information and Records Management Society's School Record Retention and Disposal Toolkit, and from this a bespoke Retention Policy has been created – see Appendix 4) The Trust and its academies will also implement measures to ensure the annual review of records against the retention schedule as outlined in the Retention Policy.

Upon leaving the Trust, pupil files, both electronically via the school to school service, and paper-based should be transferred to the new school, or given back to the LA if the pupils are leaving the country or moving to a private school.

Security

All employees are responsible for ensuring that data security is maintained in line with the following requirements, the wider Information Governance Policy (IGP), and any related Academy policies and procedures.

The Trust and its Academies will ensure that appropriate technical and organisational measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data, as follows:

- See the Information Security Policy below for technical measures to be followed.
- All employees will read and sign to state they will comply with the ELT Acceptable Use Policy – See Appendix 5. This will be reviewed annually, with renewed signatures required.
- Organisational measures:
    - Each Academy will define an Access Control Policy – see Appendix 6 for Template, outlining the roles within the Academy and the systems, applications and information they need to access in order to fulfil their role.
    - Paper records must be kept in a locked filing cabinet, drawer, or safe, and only made available where there is relevant/appropriate purpose to do so.
    - If personal data is held on a laptop, mobile device or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or otherwise secured when not in use.
    - Lock computers if logged in when leaving the computer for any short period of time (a maximum of 5 minutes is advised)
    - Log out the computer if logged in when leaving it for an extended period of time (more than 30 minutes is advised)

- When viewing personal information on screen or at your desk, consider who may be able to view the information and use the locked screen function when away from your desk.
- All employees are to work within the Home Working Policy that outlines the measures each employee needs to take to ensure secure, home working.
- At the end of the working day or when a desk will be left unattended for a period of time all sensitive or confidential documents must be secured in a lockable cupboard or desk, operating a clear desk policy.

Use of third party suppliers (Data Processors)

The procurement of third-party service providers (data processors) who will handle the Trusts personal information in the course of providing their service on behalf of the Trust or an Academy within the Trust will:

- require assurances from the data processor on how they proposed to handle the personal information – by either a letter of assurance, or contract agreement.
- result in a contract that meets the requirements of the General Data Protection Regulation and the DPO is involved throughout this process.

This will be achieved by using the following documents:

- ELT Procurement Policy and associated documents – Supplementary Policy

A Data Processing Agreement (DPA) will be signed by both parties before a contract can be entered into unless this is included in the terms and conditions of the company. Were the company act as a Data Controller a Data Sharing Agreement will be put in place. The Trust DPO will provide these documents and sign to agree the use of this service.

A log of all DPA's and DSAs will be made available to academies using a log which is kept up to date on OneDrive under GDPR – Academies.

As part of the DPO termly audits checks will be made to ensure that the appropriate documentation has been signed before the system or service has been implemented.

Data Protection Impact Assessments

When the need for a new system and/or service is identified, either by an academy or the Trust, the following must apply:

- A clearly defined rationale for commissioning a new system or service is shared with the Director of Business and Operations – includes proposal, estimated cost, benefit and desired outcomes.
- If the new system or service involves the sharing, processing or storage of data then a Data Protection Impact Assessment is completed and submitted to the Trust's Data Protection Officer and Director of Business and Operations.
- This information will be reviewed by the Information Governance Strategy Group for a recommendation. All recommendations from the Information Governance Strategy Group will be sanctioned by the Finance, Risk and Audit Committee.
- If the decision is to proceed with the procurement, the Central Team will conduct the process in line with this policy and Scheme of Delegation.

- As part of due diligence, a Request for Quotation will be available to prospective bidders setting out the specification, timeline, evaluation criteria and conditions of the award. The Request for Quotation also includes a requirement for bidders to submit policies and procedures relating to Data Protection and Health and Safety, method statements on data security, data sharing and data processing, and a Freedom of Information Disclosure Notice.
- Any contract that involves the sharing and/or processing of data will only be let on the receipt of a Data Sharing and/or Data Processing Agreement.

Any agreement, contract or lease with a supplier must be authorised by either the Chief Executive Officer, Director of Business and Operations or the Chief Finance Officer. This does not include general orders for goods and services.

All IT purchases must involve the Director of Information and Technology.

A signature on an agreement or contract, or even an email response indicates that the Trust or Academy accepts the suppliers Terms and Conditions which may not be favourable and/or in line with this policy.

Sharing

All employees must contact their Principal or Business Manager for advice before releasing any personal information if they are unclear about the procedures or protocols to follow.

Employees must:

- Be able, if asked, to justify their sharing of personal information
- Maintain security to the level expected by the classification of the personal information, whether the sharing is in person, made verbally, by email, fax, or post.
- Not use removable media devices – such as USB drives or memory sticks – to share information.
- Where information can me anonymised, use pseudonymisation techniques with unique identifiers so that the identity of the people within the information you're sharing, is hidden, or if possible, redact completely.

In all cases, follow the steps below:

Before sharing or sending the personal information

Be satisfied

- Of the identity of the recipient; this includes both internal colleagues, external third parties and individuals.
- Of the contact details of the recipient – e.g. email address; fax number; phone number.
- Of the recipient's need to know and/or their entitlement to the personal information – seeking written proof where necessary.
- That they are authorised to share the personal information.
- If in doubt, the personal information should not be shared. Instead, further details and assurance must be sought. For example,
    - Return the intended recipient's call using a known telephone number.
    - Verify the intended recipient's email address by checking against a known source.
    - Verify the intended recipient's postal address by checking against a known source (e.g. seeking copies of formal, official headed documentation).

Always consider the amount of information to be shared, and that what is being shared is factual.

The personal information to be shared must

- Only be that required to fulfil the purpose or purposes behind the proposed sharing, or
- Only be that defined on any court order or other document compelling disclosure, and otherwise be accurate.

A secure means of disclosure must be used

Employees must protect the interests of the individuals subject to the personal information – for example, their confidentiality and privacy – and The Trust's interests when

Disclose information by email

- Emails are encrypted when containing personal or confidential information. When sending emails to Trust or ELT academies, all emails will automatically be encrypted if the academy is on the Trust email platform.
- Sending emails outside of the organisation when the academy is on the Trust email platform must have ENCRYPT: prefix in the email Subject to enforce encryption.
- Sending emails outside of the Trust must be encrypted using 3rd party software should the content be of a confidential nature and academies aren't on the Trust email platform.
- Emails being sent are checked to ensure recipients addresses are correct, and valid

Disclose information by post

- Post containing personal or confidential information is sent Recorded or Special Delivery
- Recipients addresses are checked to be correct and valid before sending any post
- Post that is sent Recorded or Special Delivery is recorded on an internal system in case of loss, or delivered in error

Disclosing information verbally

- Discussing personal information in conversations,
- Using telephones or
- Recording information on voicemail, answering machines, video or audio devices.

Employees must:

- Use any private offices, rooms or spaces provided by the Trust and/or their Academy, or
- Otherwise take due care to ensure they are not overheard by anyone who has no need to access the information being discussed. For example, calls must not be made or taken in confined public places or on public transport.

Disclosing information by Fax

At the end of each day, a named role within the office will review the fax logs to check for compliance, errors and send failures, and take appropriate action where required.

- Always use a Fax Cover / Header Sheet. The Sheet must include the following five details: the Recipient; the Sender; their contact details; the number of pages; the

following disclaimer: The information contained in this fax is Strictly Confidential and is intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender. This will ensure that, should a fax be misdirected, the person receiving the fax will know who sent it and has clear instructions on what to do with the fax.

- For occasional faxes, use the 'Call and Confirm' approach, as follows:
    - Double check the correct dialling code and current fax number – by checking with the recipient.
    - Enter the number and double check before sending.
    - Confirm when someone will be available to receive the fax – do not send if the recipient is not there to receive the fax.
    - Call the recipient once the fax has been sent (or agree that they will call or email you) to confirm safe receipt of all pages of the fax.
    - If the fax is not received, check the number dialled. Report any delivery failures to your manager.

- For frequently used fax numbers, use the 'Pre-programmed' approach, as follows:
    - Pre-programme the frequently used fax number into the fax machine.
    - Always use the pre-programme number – do not enter the number manually.
    - Completed steps c.–e. of the 'Call and Confirm' approach above.

Disclose information by Online/FTP site

- Any requests to share personal or confidential information via online means, or FTP upload sites are checked with the Trust's Director of Information Technology for compliance first
- Confirmation from recipients is required upon sending any data via online methods to ensure they themselves have received this and no-one else in error.

Sharing Exemptions

Were possible individuals should at least, be aware that personal data about them has been or is going to be shared – event if their consent for the sharing is not needed. However, in certain limited circumstances the Data Protection Act 2018 provides for personal data, even sensitive data, to be shared without the individual even knowing about it.

You can share without an individual's knowledge in cases where, for example, personal data is processed for:

- The prevention or detection of crime:
- The apprehension or prosecution of offenders;
- The safeguarding of a child or individual; or
- The assessment or collection of tax or duty.

Information Classification

The Trust understands that our academies need to retain and dispose of records in accordance to current guidance and legislation. The guidance below will help you around best practice:

As a minimum, personal data includes all data falling in to either category A or B below:-

Category A - Any information that links one or more identifiable living person with private information about them.

There should be restrictions on a data set that includes:

- One or more of the pieces of information through which an individual may be identified i.e.
- Name
- Address
- Telephone number
- Driving licence number
- Date of birth
- Photograph

Combined with:

- Information about the individual whose release could harm or distress, including:
- Bank/financial/credit card details
- National Insurance number
- Passport number/information on immigration status
- Tax, benefit or pension records
- Place of Work
- Academy attendance / records
- Material related to social services (including child protection) or housing case work
- Conviction / prison/ court records/evidence
- Groups/affiliations/politics, race, religion, trade union, health, sexual life as defined by the Data Protection Act (Section 2)

Information Risk Register & Action Plans

Each academy and the Trust identify the information and systems used that hold personal and/or sensitive information. This is recorded onto an Information Risk Register – See Appendix 13 (previously Data Mapping Template), and from this create an Action Plan – See Appendix 14 which allows us to:

- Review the register and action plans annually, or when new systems are implemented
- Ensure the following details are recorded, and that the people involved in the use/processing of the system/information, are aware of their responsibilities:
    - Type of information
    - Department

- Data types
- Where is it stored
- Who has access
- Retention period
- Disposal method
- Data processors involved

- Check compliancy in regards to storage, access, retention and disposal as outlined in the Information Risk Register and Action Plans

The Trust will audit each academies' Information Risk Register and Action Plans annually, and/or via the Trust DPO's scheduled audits, and raise any concerns direct to the academies and IG Strategy Group to resolve within agreed timescales, as well are reviewing and auditing our own central Information Risk Register and Action Plans.

Category B - Any source of information about 100 identifiable individuals or more, other than information sources from the public domain.

This is a minimum standard. Information on smaller numbers of individuals may justify restricted value because of the nature of the individuals, source, or extent of information.

Information is classified as being one of the following:

Classification	Definition / Risk	Risk	Example	Access Method	Disposal
Public	Information clearly of interest to the public and in the public domain	No risk to the Academy or individual	Academy prospectus Academy holiday dates General letters home Information also held on Academy Website	Anonymous, no authentication required	
Internal	Information that is considered to be of no interest to the public and that is not published	No risk to the Academy or individual	Department minutes Tracking sheets Internal process documents	Username and password	Secure disposal (paper based) Hardware disposal through appropriate channels and with support from ICT provider (computer based)
Personal Data	Likely to cause some discomfort, stress, embarrassment or financial loss to an individual or embarrassment to Trust/Academy.	Likely to cause prolonged distress to many people Likely to cause serious risk to any parties personal safety.	See Definition of Personal Data Sims Reports	2 levels of authentication – different usernames & passwords or Remote Working access	Secure disposal (paper based) Hardware disposal through appropriate channels with support from ICT provider (computer based)
Confidential	Information that could seriously undermine the organisation, damage security, operations, finance of economic and commercial interest	Likely to cause a serious crime prosecution to collapse. Likely to cause a financial loss to the Trust/Academy in excess of £10,000 Likely to cause a serious illness or injury to any party Likely to cause loss of reputation for the Academy	Payroll details Department self evaluation reviews Banking details Bids/Tenders Employment records i.e. disciplinary	2 levels of authentication – different usernames & passwords or Remote Working access	Secure disposal (paper based) Hardware disposal through appropriate channels and ICT provider (computer based)

Subject Access Requests and other disclosures

Subject Access Requests

All employees, parents and other users have a right to access personal data being kept about them. Parents may also wish to submit requests on behalf of their child.

Subject Access Requests can be made verbally or in writing. Please follow the Subject Access Request Checklist, see Appendix 7.

An Academy Principal will, upon receipt of a verbal or written request,

- Inform the DPO of the request within 24 hours of receipt of the request
- Acknowledge receipt and confirm any additional information or payment that may be required in order to process the request.
- Process the request in accordance with the Subject Access Request checklist, see Appendix 7.
- The proposed response and any concerns about disclosing this information is then shared with the Trust's DPO within 30 calendar days.
- Confirmation to proceed will be given from the Trust's DPO within the 30 calendar day period.

The Trust/Academy aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within the statutory 30 calendar day timescale.

The DPO of the Trust Directors team will maintain a log of all Subject Access Requests, which is automatically updated upon each request being entered by online Microsoft Forms, to monitor compliance with the requirements of the Data Protection Act, including the statutory 30 day response timescale. All SAR requests made during school holidays should be forwarded to the Trust DPO to action.

Other disclosures

Requests made by other organisations will be subject to the checks outlined in the Sharing section outlined previously.
All disclosures must be shared with the DPO within 24 hours of receiving the request. A log will be kept centrally by the DPO and reported to the IGSG monthly.

Publication of Academy Employees Personal Information

Certain items of personal information relating to academy employees will be made available via searchable directories on the public Web site, and may be disclosed in response to Freedom of information requests, in order to meet the legitimate needs of researchers, visitors and public interests in transparency. See the Freedom of Information Policy below.

Processing in line with other individual rights

In addition to Subject Access, the Trust and its Academies recognise all individuals have the following rights

- Prevent the processing of data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause unwarranted substantial damage or distress.
- Object to any decision that significantly affects them, being taken solely by a computer or other automated process.

All requests by individuals to user these rights should be directed to the DPO of the Trust Directors team

Reporting of actual or suspected breaches

All employees are responsible for notifying the Principal if there is an actual or suspected breach of the IGP.

- On finding or causing a breach, or potential breach, the employees or data processor must immediately notify the Principal and DPO, within 2 hours, this allows for cover to be arranged for teaching staff
- All breaches or potential breaches must be recorded via the 'Data Breach Form' which can be found on the Trust intranet
- Data processors must adhere to timescales set out and agreed to in the SLA's/Contracts/DPA's signed up to.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Principal and CEO of the Trust
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant employees 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 assess the risk with the Principal to decide 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 including Safeguarding, Child Protection, and personal and sensitive information of both employees and pupils.
    - Discrimination
    - Identify theft or fraud
    - Financial loss

- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO with 72 hours.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's secure file server.

- 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 See Appendix 9 – Breaches Checklist:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored and maintained automatically by Microsoft Forms upon completion by the school and will be monitored by the DPO.

The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. A record of any recommendations will be kept by the DPO and shared with the Principal and IGSG.

Data Protection Officer

Liz Thompson is the Trust's Data Protection Officer will undertake the following tasks, and will be first point of contact for all Academy's in reference to all Data Protection related queries, and will:

- Ensure all academies are sufficiently trained to follow the Trust's Information Governance and related policies.
- Inform and advise the Trust, its academies and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train employees.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).
- Conduct internal audits and spot checks using the following process and documentation:
    - Academies will be identified on a termly basis by the IGSG,
    - Academies will be informed 1 week prior to the audit
    - Audits will take place on an annual basis for each academy unless the audit highlights areas of significant concern
    - The DPO will share the audit report with the IGSG and Principal within one month of completion
    - The academy will have to produce an revised GDPR Action Plan which will be agreed by the IGSG
    - The audit will cover a range a topics in relation to the Information Governance Policy

Contact details for our Data Protection Officer, are:
Mrs Liz Thompson - Liz.thompson@enquirelearningtrust.org - 01924 792960

The Deputy DPO is Mr Paul Kennedy – paul.kennedy@enquirelearningtrust.org - 01924 792960

Trust Level Reporting

Monthly

The DPO will report monthly to the IGSG on:
Data Breaches
Near misses
FOI
SAR
Feedback on internal DPO audits
DPIA's will be submitted monthly for approval from the IGSG, feedback is given to the academy following the decision from the IGSG.

Termly

The Audit, Risk and Finance committee receive the minutes from the IGSG.

Where a serious breach is reported the DPO will inform the Trustees directly.

Annually

The DPO reports annually to Trustees on the KPI's.
The IGSG will review a random selection of DSA and DPA to ensure that the correct process has been followed.

3. Induction, Training and Awareness Overview

The Trust have a set Induction Policy (Supplementary Policy) in place that has been developed to ensure that all employees new to the Trust (or those moving in to new roles) receive a full and thorough induction and introduction to the organisation and individual academy. The Induction Policy should be read in conjunction with the employees handbook.

In order to ensure structure to the induction process, the policy includes a checklist that is broken down in to stages so that employees receive a gradual flow of information.

The Trust and Academies will ensure that all employees who handle personal information receive sufficient training in data protection and freedom of information. This training will be based on the volume and sensitivity of personal information their role is required to handle, and the frequency with which they handle such information. The level of training required will be dependent on the individual role will be reflected in the learning journey on the Trust's e-learning package.

Termly training for Principals and Academy Business Managers will be delivered by the DPO in relation to specific areas of the IGP. Annual external training delivered by the Trust's legal team takes place during the summer term. The focus for the training will be agreed by the IGSG on a monthly basis following feedback from the DPO audits and other information available, such as the number of data breaches, SARs or FOIs – See Appendix 12 for Training Schedule

All employees will be made aware of and understand the IGP and related policies and procedures and will undertake refresh policy awareness training every 12 months as a minimum. This training will take place in September during and INSET Day.

Supply and agency staff members will be provided with a privacy notice specific to their role whilst in school. This document will provide sufficient details around Information Governance, school policies and processes and who to contact with any questions or concerns around information governance and data protection. Supply and agency staff members are not expected to share any personal or confidential information at any time, save with relevant employees of the academy.

Academies are required to maintain sufficient records to enable the Trust to demonstrate that each employee has;

- Signed and agreed their terms and conditions (contracts) of employment;
- Completed their induction checklist within the Induction Policy

- Completed their annual policy declaration (ALL employees); See Appendix 8
- Completed mandatory data protection training, and
- Completed any further training, as required by the role.

Further information on the Trust's process for induction can be found in the Induction Policy, and any queries can be raised with Human Resources.

4. Information Security Policy

Mandated ICT Infrastructure

With affect from September 2016, all Academies must adopt the following ICT infrastructure:

1	Microsoft Licensing	Windows 7 and Office 2013 minimum. Windows 10 and Office 2016 preferred.
2	Anti-Virus	Sophos Cloud deployed per academy. Endpoint and Intercept X clients to be on all devices
3	Content Filtering	SmoothWall web filter.
4	Remote Working	Must be undertaken using the Trust RDP servers for secure remote access from home See 5.3 below. Direct Access also available for users with Trust owned devices
5	Email	Cloud based via Microsoft Office 365.
6	Backups	All data is backed up daily to the Trust's secure data centre via Microsoft DPM.
7	Mobile Device Management	Lightspeed MDM implemented to lock down and control the use of iPad and other mobile devices when in the Academy.
8	Firewall Security	FortiGate firewalls consistent in every Academy, configured uniformly to block attacks on the network and allow approved content through. Trust data centre protected by Palo Alto firewalls, co-managed by Aspire Communications.
9	Remote Management & Reporting	All centralised ICT infrastructure and key software such as Office 365, SIMS and Anti Virus will be monitored and automatically reported on to the Trust's Director of Information Technology

Transitional arrangements

Upon conversion, all academies will undertake a change to immediately implement the Trust's Operational Services.

Director of Information Technology of the Trust Directors is responsible for managing transitional arrangements and will report progress to the Trust Directors and Board of Trustees.

All Academies will adhere to the Operational Services within three months of joining the Trust.

Remote working and Bring Your Own Device (BYOD)

Only Trust-owned devices should be used to access the Trust network remotely. All information must be stored on the network.

Trust-owned devices will be configured to the following minimum standard:

- Windows 7 minimum – preferred Windows 10
- Office 2013 minimum – preferred Office 2016
- Mac OSx – latest version available
- BitLocker Encryption for Windows devices, and FileVault encryption for Mac devices
- Sophos Cloud EndPoint and Intercept X anti-virus with latest updates
- Latest operating system updates applied
- Bound to the Trust domain where possible
- Added to MDM where appropriate

No non-Trust devices (i.e. personally-owned devices) should be used on-premise to access the network or to store Trust data.

The Trust realises that access to the email system on personal devices is required. To ensure that access to the email system is done securely, the following policies will be put upon any personal device:

- A password or passcode to access the device will be enforced
- The ability to remote wipe a device upon loss or theft will be made available
- A review of which employee can access email via this method will be undertaken to ensure that the risk of loss of confidential information is reduced, and Trust/Academy owned devices may need to be assigned where needed

Passwords & Responsibilities

Policy for all Employees

All Employees must follow the controls below at all times:

- Never reveal passwords or PIN numbers to anyone – including external ICT employees and their managers.
- Never use the “remember password” function on devices other than your own.
- Never write passwords or PIN numbers down or store them where they are open to theft.
- Never store passwords or PIN numbers in a computer system without encryption.

Strong passwords

All employee passwords must:

- Be a minimum of eight characters long.
- Include three of the following:
- Uppercase character.
- Lowercase character.
- Number.
- Special character.
- Not include proper names.
- Not include any part of the Employee’s username.

Director of Information Technology's responsibilities

Director of Information Technology of the Trust Directors will ensure the following measures are enforced by the following Networks, System and Applications:

Measures:

- Passwords must comply with 5.4.2 Strong Passwords above.
- Passwords must be changed every 90 days.
- The last three passwords cannot be re-used.
- The account will "locked out" following four successive incorrect log-on attempts
- Password characters will be hidden by symbols.

The Director of Information Technology is the owner of the Information Security Policy and is responsible for ensuring all academies, and the Trust have appropriate technological measures in place to adhere to what is outlined within it.

Networks, System and Applications:

Active Directory – access to all Trust network data
SIMS
Office 365 – email
Google Apps for Education – all services other than email
Sage
Trust Intranet
Web Filtering and Monitoring applications
MDM solution

Any changes – i.e. due to the functionality of Systems or Applications – will be documented and the potential risk assessed by the Director of Information Technology of the Trust Directors before being implemented.

Academy ICT responsibilities

Where not covered by the Director of Information Technology's responsibilities above, each academy shall ensure its ICT adheres to the following minimum standards:

Ensure that log-on procedures are secure and do not provide unnecessary information (i.e. that could enable unauthorised access or detail the level of access that the login ID provides) for example, provide clues about valid User IDs; the operating system version (and therefore its vulnerabilities) or that the person has administration rights.

Ensure that secure authentication methods are used to access the ICT network and security infrastructure, server and client operating systems and corporate systems such as internet and e-mail.

Ensure that new accounts are created with a temporary password which the user is required to change at first logon.

Ensure that the initial password for an employee account will only be given to the new employee.

Ensure that the login procedure is also protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised employees are allowed.

Ensure than when leaving your device, it is either locked, or logged out

Ensure all successful and unsuccessful log-on attempts should be logged and monitored.

Ensure System Administration passwords are always available to a senior, nominated officer within Academy who is separate to the System Administrator(s), for example the Principle.

Ensure Operating System access control should apply to all computers and devices that have an operating system e.g. servers, PCs, laptops, tablets.

Ensure Operating System and network domain log-on procedures should also include an enforced “User acknowledgement” statement, confirming compliance with the IGP and Acceptable Use Policy.

Backups

Each Academy must comply with the Operational Services remit from the Trust to ensure that adequate backups are taken, both onsite and offsite.

All backups performed are securely taken over the Internet to a secure off site data centre and are encrypted, and would contain all school data, including information pertinent to the running of the Academy. i.e. SIMS data

Sharing via Email

When sharing information over email, please follow the process below:

- Emails are encrypted when containing personal or confidential information. When sending emails to Trust or ELT academies, all emails will automatically be encrypted if the academy is on the Trust email platform.
- Sending emails outside of the organisation when the academy is on the Trust email platform must have ENCRYPT: prefix in the email Subject to enforce encryption.
- Sending emails outside of the Trust must be encrypted using 3rd party software should the content be of a confidential nature and academies aren’t on the Trust email platform.
- Emails being sent are checked to ensure recipients addresses are correct, and valid

If you're asked to share information via any other system, authorisation from the Trust's Director of Information Technology is required before proceeding.

5. Freedom of Information Policy

Anyone can submit a request for information held by the Trust and its academies using the Freedom of Information Act.

The Trust and each Academy should provide an accessible, simple means by which someone can submit a Freedom of Information request – for example, a page on a website with contact details of either the Academy Principal and/or the DPO of the Trust Directors team.

An Academy Principal will, upon receipt of a request, will

- Inform the DPO of the Trust Directors team of the request within three working days of receipt of the request.
- Acknowledge receipt.
- The information requested is then found and compiled at Academy level.
- The proposed response and any concerns about disclosing this information is then shared with the Trust's DPO within 18 working days.
- The Trust's DPO will respond to all FOI Requests within 20 working days. Where requests are online the academy will not provide a response until they have shared the details with the DPO to be approved.

The Trust/Academy aims to comply with requests for access to personal data where it is appropriate and lawful to do so. This will be within 20 working days and must be responded to by the Trust DPO.

The DPO of the Trust Directors team will maintain a log of all Freedom of Information Requests to monitor compliance with the requirements of the Freedom of Information Act, including the statutory 20 working day response timescale.

The Trust will adopt the Information Commissioner's Model Publication Scheme version 1.2 20151023 See Appendix 10 for a copy of the scheme.

6. Records Management Policy

The Trust will adopt the IRMS file plan for use across the Trust and its academies. This file plan has been specifically adapted to ensure its relevant to the information we control and process within Enquire Learning Trust. This will be structured according to the functions of the Trust and academies – see Appendix 4 – Data Retention Guidance

The Trust will become an IRMS member to ensure the most up to date guidance is available to all its academies. Each time a new version is released, the Trust relevant version of this will be adapted and provided to academies.

Each academy will keep a log of information that has been disposed of, the date, method, and any receipts from 3rd party contractors used.

The Trust have already mandated that a Finance File Plan is put in place per academy. In addition to this, the IRMS guidance can be used to ensure that all other records that are kept, are done so in accordance to this legislation.

The Record Management Policy and associated File Plans will be reviewed periodically.

The Trust offer guidance on the preferred File Plan for personnel records. A copy of the personnel file checklist and associated guidance document is available from Human Resources.

Appendices

1. Website Privacy Statements – for parents and pupils
2. Multiple use Consent Form
3. Accurate Record Keeping Guidance
4. Data Retention Guidance
5. ELT Acceptable User Statement
6. Access Control Policy, Guidance, Checklist and Log Template
7. Model Data Protections Clauses
8. Subject Access Request Checklist, Log and Request Form
9. Induction Checklist and Statement of Understanding
10. Security Breach Checklists, Template Log and Letter
11. Freedom of Information Model Publication Scheme
12. Employee Privacy Statement