Information Governance Policy

1. Introduction

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:

1.1. Governance and Compliance – i.e. the actions the Trust and its Academies will undertake to ensure compliance with the IGP.

1.2. Data Protection Policy – i.e. the confidentiality, integrity and availability of personal data and sensitive personal data relating to governors, staff, pupils, and parents / carers.

1.3. Information Security Policy – i.e. the technical and organisational measures to be adopted by the Trust to manage the security of information.

1.4. Freedom of Information Policy – i.e. managing public access to information created and held by the Trust.

1.5. Records Management Policy – 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
- Home Working
- Social Media
- Induction Policy

2. Document 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

3. Governance and Compliance

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

3.1. 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.

3.2. Trust Leadership – i.e. central support team

The Trust Leadership will allocate a role to be responsibility 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 staff and/or the public.
- The *Data Protection Officer (DPO)* will be allocated this role.

3.3. Academy Principal (Level 3)

The *Principal* or *Vice Principal* 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* or *Vice Principal* will report on their Academy's compliance with the IGP to the Trust Leadership as required by the Trust Leadership.

3.4. All staff

The Trust and all staff 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.

3.5. Status of this policy

The IGP does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust and academies from time to time. 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 are deemed to constitute gross misconduct

3.6. 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 Trust Leadership, and updated whenever a new Academy joins the Trust.

4. Data Protection Policy

4.1. General statement

The Enquire Learning Trust and its academies need to keep personal data about its employees, students and other users to allow it to monitor performance, achievements, health and safety, to process data so that staff can be safely recruited and paid, to manage the professional development of staff 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 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. See 4.2.
- **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. See 4.3.
- **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. See 4.4.
- **Sharing**: share information with others only when it is legally appropriate to do so. See 4.5.
- **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. See 4.6.
- **Training and Awareness**: ensure our staff are aware of and understand our policies and procedures. See 4.7.
- **Reporting of Actual or Suspected Breaches**: ensure the Trust is aware of an actual or suspected breaches of the IGP, in order than it can quickly assess the situation and take actions to reduce any risks. See 4.8.

4.2. Transparency

4.2.1.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.

4.2.2.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.

4.2.3.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 school purpose – see Appendix 2.

4.2.4.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 12.

Systems that will be monitored by the Trust are:

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

4.2.5.Use of staff information

The Trust and its Academies will process data about staff for legal, personnel, administrative and management purposes in order to enable it to meet its legal obligations as an employer, for example to compensate staff, monitor performance and to confer benefits in connection with employment.

The Trust and its Academies may process sensitive personal data relating to staff including, as specified within the Trust's Employees Privacy Statement – Appendix 12.

4.3. Quality

4.3.1.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.

4.3.2.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 staff 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 staff member has informed the academy of such changes.

- All staff are responsible for maintaining accurate records about other people – e.g. about a student's home work, opinions about ability, references to other academic institutions, or details of personal circumstances – they must follow the Trust's "*Accurate Record Keeping Guidance*" – see Appendix 3

4.3.3.Data retention

The Trust and its Academies have a duty to retain some staff 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 – see Appendix 4), and implement measures to ensure the annual review of records against the retention schedule.

4.4. Security

All staff 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 staff will read and sign to state they will comply with the ELT Staff 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 school 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.

4.4.1.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:

- 'Procurement – Model Data Protection Clauses' – see Appendix 7
- 'Procurement – Trust Finance Policy

4.5. Sharing

All staff 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. Staff 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.
- in all cases, follow the steps below:

4.5.1.Before sharing or sending the personal information

Be satisfied

1. of the **identity of the recipient**; this includes both internal colleagues, external third parties and individuals.
2. of the **contact details of the recipient** – e.g. email address; fax number; phone number.
3. of the recipient's **need to know and/or their entitlement to** the personal information – seeking written proof where necessary.
4. 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,

a) Return the intended recipient's call using a known telephone number.

b) Verify the intended recipient's email address by checking against a known source.

c) Verify the intended recipient's postal address by checking against a known source (e.g. seeking copies of formal, official headed documentation).

4.5.2.Always consider the amount of information to be shared.

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.

4.5.3.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

4.5.3.1. Disclose information by email

i. 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.

ii. 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.

iii. 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.
iv. Emails being sent are checked to ensure recipients addresses are correct, and valid

4.5.3.2. Disclose information by post

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

4.5.3.3. Disclosing information verbally

i. discussing personal information in conversations,
ii. using telephones or
iii. recording information on voicemail, answering machines, video or audio devices.

Employees must

iv. use any private offices, rooms or spaces provided by the Trust and/or their Academy, or
v. 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.

4.5.3.4. 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, reducing the risk that Whizz-Kidz will be unaware of the incident and are able to take steps to reduce the impact.

For occasional faxes, use the 'Call and Confirm' approach, as follows:

a. Double check the correct dialling code and current fax number – by checking with the recipient.
b. Enter the number and double check before sending.
c. Confirm when someone will be available to receive the fax – do not send if the recipient is not there to receive the fax.
d. 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.
e. 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:

a. Pre-programme the frequently used fax number into the fax machine.
b. Always use the pre-programme number – do not attempt to enter the number manually.
c. Completed steps c.–e. of the 'Call and Confirm' approach above.

4.5.3.5. Disclose information by Online/FTP site.

i. 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

ii. 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

4.5.3.6. 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:

What information is classed as "Personal Data"?

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 that individual whose release could cause 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
    - School 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)

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 of the information, 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 school or individual	School prospectus School holiday dates General letters home Information also held on School 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 school 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/school.	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/school in excess of £10,000 Likely to cause a serious illness or injury to any party Likely to cause loss of reputation for the school	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)

Please understand that the references in the table above are only some examples of types of information you may currently keep. For any items not listed, and you'd like guidance around how to dispose, please contact the Trust's DPO

4.6. Subject Access Requests and other disclosures

4.6.1.Subject Access Requests

All staff, 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.

Any person who wishes to exercise this right should complete the Subject Access Request Form, see Appendix 8, and submit it to the Academy Principal and/or the DPO

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

- Inform the *DPO* of the request within three working days 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 8.
- 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 statutory 30 calendar day timescale.

The *DPO* of the Trust Leadership team will maintain a log of all Subject Access Requests, see Appendix 8, to monitor compliance with the requirements of the Data Protection Act, including the statutory 30 day response timescale.

4.6.2.Other disclosures

Requests made by other organisations will be subject to the checks outlined in **Section 4.5 Sharing** outlined above.

4.6.3.Publication of Academy Staff Personal Information

Certain items of personal information relating to academy staff 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.

4.6.4.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 Leadership team

4.7. Induction, Training and Awareness Overview

Our Induction Policy has been developed to give new employees an introduction to the Enquire Learning Trust and should be read in conjunction with the staff handbook. The purpose of this programme is to help you to settle into your new job as quickly and smoothly as possible.

Your first few weeks will be spent getting to know the academy, meeting the people you will be working with and learning about your new job and how you will contribute to the overall effectiveness of the Trust.

Your manager will also want to find out more about you and your needs at work. This is to ensure you are supported as much as possible from a welfare perspective as well as your professional development.

In order to add structure to this process, the induction programme is based on a check list. The check list is broken down into stages so that you receive a gradual flow of information. If at any stage of the process, you feel that you are not getting the information and input you require, you should discuss this with your manager in the first instance.

A number of different people have a role in ensuring your induction programme is completed successfully. Your line manager will make the arrangements for you to meet with the relevant people in order to complete the induction programme. The people you need to meet with will vary dependent on your role and as such your line manager will discuss this with you when you begin the process.

The Trust and Academies will ensure that all staff who handle personal information received sufficient training in data protection and freedom of information – based on the volume and sensitivity of personal information their role is required to handle, and the frequency with which they handle such information.

All staff will be made aware of and understand the IGP and related policies and procedures.

The Trust (HR) and the individual Academies will 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 (new starters); See Appendix 9
- completed their annual policy declaration (existing employees); See Appendix 9
- received Employee Privacy Statement; See Appendix 12
- completed mandatory data protection training, and
- completed any further training, as required by the role.

4.8. Reporting of actual or suspected breaches

All staff 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 staff member or data processor must immediately notify the Principal and DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the 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 staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored 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 10 – 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 by the DPO on the Trust secure file server

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

4.9 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 schools 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 staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Contact details for our Data Protection Officer, are:

Mrs Liz Thompson

Liz.thompson@enquirelearningtrust.org

01924 792960

5. Information Security Policy

5.1. 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	Onsite to NAS hosted in alternate location to server in case of theft, fire or leak, and offsite backup for key data – SIMS etc…
7	Mobile Device Management	Lightspeed MDM implemented to lock down and control the use of iPad and other mobile devices when in school.
8	Firewall Security	FortiGate firewalls consistent in every school, 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

5.2. 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 Leadership* is responsible for managing transitional arrangements and will report progress to the Trust Leadership and Board of Trustees.

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

5.3. 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-premiss 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 staff 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

5.4. Passwords

5.4.1.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 staff 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.

5.4.2.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.

5.4.3.Director of Information Technology's responsibilities

Director of Information Technology of the *Trust Leadership* 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.

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 Leadership* before being implemented:

5.4.4.Academy ICT responsibilities

Where not covered by 5.4.3 *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.

5.5. Backups

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

On site backups will be taken to a NAS that will be located in school, but not in the same location as the server, in case of fire, flood or theft

Off site backups will be taken to a secure cloud storage location, encrypted, and would contain information pertinent to the running of the school. i.e. SIMS data

6. Freedom of Information Policy

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

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

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

- Inform the *DPO* of the Trust Leadership team of the request within three working days of receipt of the request.
- Acknowledge receipt.
- The information requested is then found and compiled at school level.
- The proposed response and any concerns about disclosing this information is then shared with the Trust's DPO within 18 working days.
- Confirmation to proceed will be given from the Trust's DPO within the 20 working 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 statutory 20 working day timescale.

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

The Trust will adopt the Information Commissioner's Model Publication Scheme version 1.2 – 23rd October 2015 - See Appendix 11 for a copy of the scheme.

7. Records Management Policy

The Trust will adopt the IRMS file plan for use across the Trust and its academies. 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.

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.

To implement the Trust preferred File Plan, please liaise with Human Resources in the first instance.

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 Staff 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. FoI Model Publication Scheme
12. Employee Privacy Statement