ACKLAM GRANGE SCHOOL

Data Protection Policy 2020-2021

	Term	Year
Last Review Date/Policy Adopted	Autumn Term	2019
Next Review Date	Summer Term	2021
Lead	A Crawshaw / N Flint / M Lodge	

This school is an academy within The Legacy Learning Trust.

The Legacy Learning Trust

Data Protection Policy

Aims and Objectives:

The aim of this policy is to provide a model set of guidelines to enable staff, parents and students to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and students can access personal data
- The need for information and I.T. security and their own responsibilities in this respect

The objective of the policy is to ensure that the school acts within the requirements of the Data Protection Act 2018 when retaining and storing personal data, and when making it available to individuals, and that the process of responding to enquiries for other information is also legal under the Freedom of Information Act 2000 (in force from 1st January 2005).

Data Protection – the law:

Under the Data Protection Act 2018, and other regulating acts, access to their own personal information is a statutory right for students (if they are of an age to understand the information they request) and parents (as defined in the Education Act 1996) may also request access to their child's personal data.

School staff have a right of access to personal data on themselves.

Anyone has the right to question and correct inaccurate information, but this must be matters of fact, not opinions.

Personal data should always be kept securely and protected by passwords if it is electronic, and access to it should only be by those authorised to see it – confidentiality should be respected. The law also provides that personal data should not be kept longer than is required.

Third party data (information about someone other than the requesting individual) should in general only be provided with their permission.

There should be a named person with overall responsibility for personal data within each school. In most cases this would be the Headteacher.

Freedom of Information Requests

A valid FOI request should be in writing, state the enquirers name and correspondence address and describe the information requested.

Important points to note:

- Requests should be dealt with within 20 days excluding school holidays.
- All staff should be aware of this process.
- A record should be kept of refusals and reasons for refusals as well as appeals, allowing the governing body to review its access policy on an annual basis.
- Expressions of dissatisfaction should be handled through the school's existing complaints procedure.

If a member of staff receives a request for information it should be forwarded to the Executive Headteacher, Ms Andrea Crawshaw, and in her absence the Director of Corporate Services, Mrs Nikola Flint.

This person would then:

- Decide whether the request is a request under Data Protection Act 1998 (DPA), Environmental Information Regulations 2004 (EIR) or Freedom of Information Act 2000 (FOIA).
- Decide whether the school holds the information or whether it should be transferred to another body.
- Inform the enquirer if the information is not held.
- Consider whether a third party's interests might be affected by disclosure and if so consult them.
- Consider whether any exemptions apply and whether they are absolute or qualified.
- Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information.
- If a request is made for a document that contains exempt personal information ensure that the personal information is removed as set out in the guidance for schools.
- Decide whether the estimated cost of complying with the request will exceed the appropriate limit.
- Consider whether the request is vexatious and repeated.

Processing, storing, archiving and deleting personal data: guidance

- Personal data and school records about students are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when students change schools.
- School records for a child should be kept for 7 years after the child leaves the school and examination records the same.
- Data on staff is sensitive information and confidential to the individual, and is shared, where appropriate, at the discretion of the Headteacher and with the knowledge, and if possible the agreement of the staff member concerned.
- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.) these records should be retained – Miss R McGurrell to advise.
- Interview records, CVs and application forms for unsuccessful applicants are kept for 6 months.
- All formal complaints made to the Headteacher or members of the Local Council will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

Accessing personal data: guidance

- A child can request access to his/her own data. The request is not charged and does not have to be in writing. The staff will judge whether the request is in the child's best interests, and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion.
- A parent can request access to or a copy of their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be a charge for photocopying records – this is detailed in guidance available from the Information Commissioner. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.
- Parents should note that all rights under the Data Protection Act to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from one child to another, but, as a broad guide, it is reckoned that most children will have a

sufficient understanding by the age of 13. Parents are encouraged to discuss and explain any request for information with their child if they are aged 13 or over.

- Separately from the Data Protection Act, The Education (Pupil Information)(England) Regulations 2005 provide a student's parent (regardless of the age of the student) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.
- For educational records (unlike other personal data; see below) access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment.
- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. There is no charge for copies of records.
- The law requires that all requests for personal information are dealt with within 40 days of receipt except requests for educational records (see above). All requests will be acknowledged in writing on receipt, and access to records will be arranged as soon as possible. If awaiting third party consents, the school will arrange access to those documents already available, and notify the individual that other documents may be made available later.
- In all cases, should third party information (information about another individual) be included in the information the staff will try to obtain permission to show this information to the applicant, with the exception of information provided by another member of school staff (or local authority staff) which is exempt from a requirement for third party consents. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.
- Personal data should always be of direct relevance to the person requesting the information. A document discussing more general concerns may not be defined as personal data.
- From 1st January 2005, when the Freedom of Information Act came into force, a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work. These can be requested if sufficient information is provided to identify them.
- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact within the data, and to ask to have inaccurate information deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.
- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request.

Definitions:

Information - Covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses etc. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.

Strong Password – A password should be a minimum of 8 characters in length, contain upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain the owner's date of birth or car registration number.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Responsibilities:

- The school is registered with the Information Commissioner's Office (ICO) under the 2018 Data Protection Act.
- The Headteacher shall inform both the ICO and the Director of Children's Services, Middlesbrough Council, if there are any losses of personal data.
- The Headteacher should record any requests or breaches on The Legacy Learning Trust School Dashboard termly return to CEO and Trust Board.
- Users shall be responsible for notifying the I.T. Service and Development Manager, Director of Corporate Services or Headteacher of any suspected or actual breach of I.T. data security.
- Users of the school's I.T. systems and data must comply with the requirements of the I.T. Data Protection Policy.
- The school's Senior Leadership Team shall review this document at least annually.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the I.T. security implications of personnel changes.
- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, tablet devices, external hard disks, memory sticks, smart phones and Personal Digital Assistants (PDAs) and other removable media.
- Remote access to information and personal data shall only be provided through an encrypted link (Ericom Access Now and Magellan) and users shall require a strong password that is renewed at least half-termly.
- Users shall not publish documents containing sensitive personal data on externally accessible web sites including the VLE (eSchools) unless these documents are encrypted.
- Users should not set web browsers or other software applications that require user authentication (internally or externally) to store or remember passwords.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Server rooms must be kept locked when unattended.
- Appropriate arrangements must be applied for the removal of any I.T. equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- All school-owned I.T. equipment and software is recorded and an Asset Register maintained.

- Uninterruptible Power Supply (UPS) units are used for servers and network cabinets.
- Users should not leave sensitive or personal data on printers, computer monitors or desk whilst away from their desk or computer, including outside school environments (e.g. home). Sensitive scanned documents should be immediately removed from the central storage area on the network (this will happen automatically at the end of each day).
- Users should not give out sensitive information unless the recipient is authorised to receive it.
- Users should not send sensitive/personal information via e-mail or post without suitable security measures being applied (Cryptshare).
- Users should ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.
- Users should not leave computers unattended. They should be 'locked' even when leaving them for a short time.

System Security:

- Users shall not make, distribute or use unlicensed software or data.
- Users must ensure they are aware of the implications of private use of the school's computer facilities.
- Passwords should be memorised. Passwords should not be written down.
- Users who regularly access personal data shall have a unique user ID and a strong password that is renewed at least half-termly. A password should be a minimum of 8 characters in length, contain upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain the owner's date of birth or car registration number.
- Passwords shall not be revealed to anybody else under any circumstances.
- Passwords shall not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- Permission is required for the deletion of folders and files where such an action may compromise the school's data systems and structures.
- Backup copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- Backup copies should be clearly marked and stored in the fireproof safe.

Virus Protection:

- The school ensures that current and up-to-date anti-virus software is applied to all school I.T. systems.
- Laptop users shall ensure they update their virus protection at least monthly by ensuring that their laptop is brought into school and logged into the network.
- Any suspected or actual virus infection must be reported immediately to the I.T. Service and Development Manager and that computer shall not be reconnected to the school network until the infection is removed.

Disposal of Equipment:

- The school shall ensure any personal data or software is erased from a computer or device if the recipient organisation is not authorised to receive the data.
- It is important to ensure that any software remaining on a PC being relinquished for re-use is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The school shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.