Elm Court School
Every Learner Matters
The Livity School

Elm Court Livity Federation Data Protection and Confidentiality Policy

1. Introduction to the Policy

This policy applies to:

- All staff (permanent, temporary, supply teaching and non-teaching, and otherwise)
- Advisors/inspectors
- Parents/carers
- The School Governors
- Students and volunteers

All schools have to keep some information confidential, digital, written and spoken. It is important that the whole school follows the same clear and explicit policy. Pupils, parents, carers and governors should be made aware of this and how it works in practice.

2. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data.
- How personal data should be processed, stored, archived and deleted/destroyed.
- How staff, parents and pupils can access personal data.
- To give clear guidance to all members of the school around confidentiality.
- To inform parents and other stakeholders about confidentiality and data protection
- To encourage staff to listen and be aware and if they have concerns over confidentiality to inform a member of the Senior Leadership Team.
- To give staff confidence to deal with sensitive issues professionally.

It is a statutory requirement for all schools to have a Data Protection Policy

3. Data Protection Principles

The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes.
- Personal data shall be adequate, relevant and not excessive.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
- Personal data shall be kept secure i.e. protected by an appropriate degree of security.
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

4. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, A similar process should take place with managing school data. The DPA defines different types of data and prescribes how it should be treated. For example, identifying what data can be freely available in the school and what may be required to be kept in a locked drawer or secure area on the network/ what personal information/data needs to be shared and with whom.

The loss or theft of any personal data is a " potential data breach" which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

5. Personal Data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:-

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, disciplinary records.

- Curricular / academic data eg class lists, pupil / student progress records, reports, references.
- Professional records eg employment history, taxation and national insurance records, appraisal records, disciplinary records and references.
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

6. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following 8 categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings. It requires a greater degree of protection and in a school would include:-

- Staff trade union details.
- Information on the racial or ethnic origin of a child or member of staff.
- Information about the sexuality of a child, his or her family or a member of staff.
- Medical information about a child or member of staff.
- Information relating to any criminal offence of a child, family member or member of staff.

Note – On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the classroom or school kitchen

7. Personal Disclosures

Disclosures from pupils or parents/carers may take place at any time. If this happens, the member of staff should discuss the issue with a senior member of staff. If pupils are disclosing information, staff should follow the Safeguarding Policy and access pupils to any appropriate communication aids to aid their disclosure without asking any leading questions pupils

Key Points:

- Pupils and parents should be reassured.
- Pupils and parents should know that staff cannot offer unconditional confidentiality.
- Pupils should be reassured that, if confidentiality has to be broken, it is purely to inform those who can keep them safe.
- Pupils and parents should be informed of sources of confidential help, for example, the school nurse, social care, GP or local young person's advice service.
- Any personal information should be regarded as private and not passed on indiscriminately (for example in the staff room).
- If a member of staff receives information that leads them to believe that there is a child protection issue, they should refer the case to a Designated Safeguarding Lead.
- Government guidance requires professionals to consult as much as possible with parents about their children when referring to another agency. In general, parents should be asked if they wish to be referred, UNLESS THERE IS REASON TO THINK THAT OBTAINING SUCH CONSENT MAY PUT THE YOUNG PERSON AT RISK.

8. **Maintaining Confidentiality**

All children, staff members and governors should enjoy privacy from gossip, the school should be fair to all in its community.
Disciplinary matters should be dealt with according to the school's own procedures and out of the eye of the wider school community, it is important that:

- Staff must not discuss details of individual cases with any person without direct professional connection to and interest in the welfare and education of the individual concerned.
- No member of staff should discuss an individual child's behaviour in the presence of another child in school.
- Staff do not enter into detailed discussion about a child's behaviour with other children or their parents.
- Governors, in particular those sitting on Discipline Committees, do not divulge details about individuals (be they staff, families or individual children) to any person outside of the meeting.
- Staff performance management will be carried out privately. Targets for individuals, named lesson observation sheets and other performance data will be in the Executive Headteacher's office and electronic records will only be available from the Executive Headteacher's computer.
- Matters of Child Protection are made known to staff on a need to know basis
- It is important that class teachers and support staff are aware of some confidential matters in order to support individuals. These staff will respect the sensitivity of such cases and not divulge information to people unconnected professionally with the individual concerned.

9. Other Types of Data not Covered by the act

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include lesson plans (where no individual pupil is named), teaching resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

10. Responsibilities

The Executive Headteacher and Governing Body are responsible for data protection.

11. Risk Management

The Governing Body will keep up to date with current legislation and guidance.

Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

12. Legal Requirements

Registration
The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: http://ico.org.uk/for_organisations/data_protection/registration

13. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter.

14. Transporting, Storing and Deleting Personal Data

The policy and processes of the school will comply with the guidance issued by the ICO

15. Information Security - Storage and Access to Data

Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems.

16. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

17. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

18. Images

- Images of pupils will only be processed and transported by use of an encrypted memory stick and permission for this will be obtained in the privacy agreement.
- Images will be protected and stored in a secure area.

19. Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

20. Retention of Data

Personal data that is no longer required will be destroyed and this process will be recorded.

21. Systems to protect data

a. Paper Based Systems

- All paper based OFFICIAL or OFFICIAL – SENSITIVE (or higher) material must be held in lockable storage, whether on or off site.
- Paper based personal information sent to parents will be checked by the Executive Headteacher before the envelope is sealed

22. School Websites

Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained

23. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data. E-mails containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the document . Egress is used between the local authorities and schools.

24. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.
In the event of a data breach the Executive Headteacher will inform the Chair of Governors.

This policy was formally adopted by the Governing Body: December 2022

Review Date: December 2023