Data Privacy Notice for Pupils and their Parents/Careers

GDPR/Data Protection Act

Our school is one of the family of schools that make up The Learning Partnership multi academy Trust. The Learning Partnership Trust is a data controller for the purposes of the Data Protection Act. The Trust through each of its schools collect personal information from pupils and their parents/ carers and may receive information about pupils from their previous school, local authority and/or the Department for Education (DfE).

The categories of pupil information that we collect, hold and share about pupils and parents include:

- Personal information (such as name, unique pupil number, unique learner number and address, school system ID photographs and telephone number)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Special Educational Needs information (such as EHCP reviews, information from specialist assessors and clinical specialists etc.)
- Other personal information including relevant medical information, provided by pupils' parents/ carers, or others who support the wellbeing and education of pupils, which it is necessary to share with the staff looking after a child to ensure their wellbeing and effective education
- Behaviour and achievement information (such as records of incidents, records of achievement awards logged by teachers)
- Assessment information (including the results of external and school assessments)
- Records of tasks set for pupils and feedback given
- Any qualifications held (for older pupils)
- Information about course choices, career aspirations post-16

We use this pupil and parent information to:

- Support pupil learning
- Monitor and report on pupil attainment, progress and attendance
- Keep children safe regarding medical conditions or emergency contacts
- Provide appropriate pastoral care
- Assess the quality of our services
- Comply with the law regarding DFE data collections and data sharing

Any decision made about an individual pupil as a result of using this personal information will always involve a member of staff and never be solely automated.

Under GDPR, the lawful bases which we rely on for processing pupil information are:

We use the data only in ways that are necessary for the education of your child and the normal functioning of the school, and we design our systems to prevent unauthorised access and to manage access appropriately within the organisation.

In some cases, we collect and use pupil information because we need to do so to protect the vital interests of pupils or staff (e.g. with the medical information we process).

Collecting pupil and parent information

The schools will collect pupil information from previous schools, from Local Authorities (e.g. Cheshire East Council/ Staffordshire County Council), from the Department for Education or from parents and carers during the admissions process. Much of this is mandatory but we will indicate on our data collection and data checking forms whether you are required to provide certain pupil information to us or if you have a choice in this.

Consent

There are some types of information that we use that are not essential for the job we do. We need consent to process:

- Biometric information* (the thumb recognition system used in the canteen)

- Photographs or videos or other information that we take to use for marketing or publicity (e.g. the school website, Trust updates or newspaper articles)

For pupils in our secondary schools, we ask parents of pupils in Years 7-11, for permission to use the information via the admissions form or, in some cases, an educational visit letter. In the case of Year 12 and 13 pupils, we will seek permission from the individuals themselves during the admissions process.

In our primary schools, consent would always be sought from one parent or carer.

If pupils do not want us to use information, a photograph or video for publicity or similar they should tell the member of staff at the time or the local school data protection officer and we will not do so.

**Further technical information regarding the biometric information is included in Schedule A, at the end of this document. It includes an illustrative example of how the data is configured for storage.*

Storing pupil and parent information

We hold pupil information for the set amount of time shown in our data retention schedule, which is available from the trust and in line with IRMS guidelines. We expect to retain most pupil information until an individual is 25 years of age. Data is normally archived or deleted securely unless we have received a specific request to delete data from an individual.

Each member of staff has received data protection training and the Trust will ensure that pupil data will be securely stored within:

- the school and trust information management system (SIMS)
- Microsoft Office 365
- lockable cabinets and offices

Cloud services

In common with most schools, we use 'cloud based' services for the storage and processing of some of the data we hold about you. In all cases we remain the data controller and we ensure the services we use are compliant with legislative requirements. We also check that the information is stored only within the UK or EU and do not routinely transfer it abroad. These services include, but are not limited to, AIS (CCTV), Alps Connect, Capita SIMS, Chartwells caterers, Employ (work experience), Doddle (Science e-learning), EvolveAdvice, FFT Aspire, Satchel One, GCSE Pod, Groupcall, SparkMaths, Microsoft Office 365, Novas, ParentPay, Pearson Activelearn, SISRA Analytics (progress and assessment analysis), UCAS. In all cases we hold a signed contract with the service provider which requires them to protect pupil information properly and only process it for the purposes we intend.

Who we share pupil information with

We do not share information about our pupils with anyone unless it is a legal requirement or we have appropriate consent from parents/carers or the individual.

We routinely share pupil information with:

- Schools, colleges or similar that pupils attend after leaving us
- Our Local Authority*
- The Department for Education (DfE)
- The primary school that you attended, to support our collaboration on school improvement.

We may, in extreme circumstances, need to also share information with organisations such as the NHS, school nurse, safeguarding agencies or the police.

** We are required under section 507B of the Education Act 1996 to pass some information about you to our Local Authority (LA) Youth Support Service for young people aged 13-19 years (25 years for pupils with a learning difficulty). We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role. We may also share data with post-16 providers to secure appropriate support on entry to post-16 education and training. Parents, or pupils if aged 16 or over, can however ask that no information beyond names, addresses and your date of birth be passed to the support service. Please contact us (via the school office, or the Student Services staff, if you wish to opt out of this arrangement or if you want to receive a copy of the information that we hold about you.*

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

The Department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Individual rights to access personal information

Individuals have the right to access their data or educational record, to ask us to correct it where it is wrong and in certain circumstances ask us to delete the data or limit what we do with it. If you want to see what data we hold about you, you can make a subject access request by contacting the school Data Protection Officer, or any other member of staff and explaining that you wish to see the data that the school holds about you. We will then provide you with access to what information we hold about you in printed or electronic copies of the data where the law requires us to do this.

If you think that we are not processing your data fairly, correctly and legally then you have the right to complain. The following options are available to you:

1. Contact the School Data Protection Officer (DPO) to discuss your concerns; most worries should be dealt with successfully by doing this
2. If you are still not happy the school has a complaints policy which is published on our website.
3. You may also contact the Information Commissioner's Office which oversees the way we process data. We would encourage you to go through the internal schools processes first, although you do not have to https://ico.org.uk/concerns/

The School DPO contact details can be found on the school website.

Further information

Further information on school policies and data protection can be found in the following link:
https://3vywr6huwat37ur611ljfqt8-wpengine.netdna-ssl.com/wp-content/uploads/GDPR-Policy2018.pdf

Data protection in Cheshire East:
http://www.cheshireeast.gov.uk/council_and_democracy/council_information/data_protection/data_protection.aspx

The Department for Education’s data sharing process and the national pupil database:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract
https://www.gov.uk/government/publications/national-pupil-database-requests-received

Guidance on how schools should protect your data:
https://ico.org.uk/your-data-matters/schools/
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Schedule A

What is a biometric algorithm?

The individual templates are encrypted using a 256 bit AES key that is built into the scanners hardware. Also the persisted file is encrypted using a different 256 bit AES key built into the matching algorithm supplied by Secugen and generated by a unique license purchased for each site. This is more secure than the ANSII and ISO standards that government department’s use as the Secugen Template is encrypted and the ANSII and ISO standards are not. The template data is useless and cannot be interpreted back into a usable fingerprint image. If this was not the case then there would be no world standards and performance measures for such technologies. The data is stored in an array in the RAM of the Biometric Controller and is also permanently stored on the hard drive of the Bio Controller to be restored in the event of a reboot.

Below is an illustrative example of a template code for an individual finger:

```
0X4177414141425141414144454151414141515415341414D415A414141414141417477454141 4C714777
346C5869656D6C574945494A764A6B42466D6837616C4E764D704F517874517A706A4A395A317849356
86C4177395366726E777645576357386C4573314B426F47443166694170675559704C763168423642682
A7043
```

The solution is secure because the matching can only be done by the individual’s consent as the finger has to be presented to the device for matching. We do not hold images of fingerprints in our system.

The technology provided for this method of identification meets with BECTA guidelines and also allows students the option to opt out of the scheme and use a PIN number instead.

Also under the data protection act the school or caterer (the originator of the data) cannot allow access to this data by anyone for any other means than for the purpose the data was collected and that is to identify an individual within the solution we supply. Any biometric data that belongs to an individual that leaves the school is purged which also is in line with the BECTA* guidelines. *[*BECTA was set up by government to lead the national drive to ensure the effective and innovative use of technology throughout learning.]*

END

August 2023
Reviewed October 2024