DPIA
Biometric Site Security System

Organisation name	Beths Grammar School
Author	Claire Archibald, Legal Director, Browne Jacobson LLP, Kathryn Walker, Operations Manager, Beths Grammar School
Version	Version 1, July 2025
Data Protection Officer	Matt Neylan
Date DPO advice given	
DPO Advice	I have reviewed this DPIA, and whilst there is high-risk processing in relation to the processing of biometric data of children and employees, I am satisfied that appropriate mitigation actions have been identified to ensure that the risk is reduced.
Is DPIA legally obliged or has this been carried out as good practice?	Legally required under Article 35 UK GDPR as processing meets definition of 'high risk' processing.
Project sign off	Chair of Finance 12th June 2025

Introduction

This section is a detailed introduction, covering some of the key risk areas. It sets a context for the project and can be understood by someone with no prior knowledge.

At an Ofsted inspection at Beth's Grammar School in May 2022 it was identified that there was a potential safeguarding issue in relation to which of the school's 1700 pupils were on site at any one time. Sixth form students are permitted to move on and off the school site over the school day, and additionally, there was no easy way to identify exactly how many or which pupils were on site before the first registration period at 8.45 am each morning, or how many remained on site at the end of the school day.

Following the inspection, there were several projects to try to improve the capture of which pupils were on site outside of registration times, including the installation of a security kiosk and revised student protocols around checking in and out of the school site. However, these projects have not proved to be effective; with one pedestrian and two vehicle entrances on the site, combined with the sheer volume of students arriving and departing at key points in the day, there is no effective or affordable way to manage this without the procurement of specialist technology.

The school commenced a project to investigate their options following the inspection outcomes. It was identified that a suitable and affordable solution was available through the installation of turnstiles at entranceways, together with the availability of technology to allow pupils to be logged in and out of the site in a quick and convenient way by presenting their finger to a scanner at the turnstile.

The trust recognises that this new processing is high risk- the personal data processed relates to children and staff and includes the processing of biometric data. Biometric data is classed as 'special category data; under the UK GDPR. Additionally, in relation to biometric processing, the Protection of Freedoms Act 2012 sets out requirements for consent and the ability to refuse biometric data processing. (Whilst individuals' actual fingerprints aren't stored on the system that will be used to match the finger being presented at the scanner to the stored data, the fingerprints collected at registration are converted into numerical code, which still constitutes biometric processing- see below for further details).

Whilst this processing is high-risk, we have identified that the new project holds several key benefits, which makes this high-risk project worthwhile. We also believe that the mitigations and controls we will put in place will reduce risk to data subjects, and that the overall aims of the project justify this processing.

This DPIA is therefore being carried out not only as we are legally obliged to conduct a DPIA where high-risk processing takes place, but it will also set out and evidence our risk assessment and mitigation process. It also supports our project plan as we change our site safety and safeguarding procedures as well as providing a record of the stakeholder engagement and compliance work that has been carried out during the procurement process.

CDVI is a supply chain (wholesaler) of the product developed by IEVO, who is the manufacturer of the system that the school will be using. Neither company will have any access to personal data, and they will be responsible only for provision of the technology and its installation. We recognise that this DPIA is not a process to be visited once, but it will provide a framework for us to continue to identify and mitigate risk throughout the whole of the processing lifecycle. Our DPO has reviewed this DPIA and provided advice on the front page. This has then been reviewed by Chair of Finance, who has reviewed the outstanding risk, the advice of the DPO and have approved this project to proceed.

Intended project outcomes

This section sets out the key objectives, and how processes and outcomes for affected data subjects will be improved. It is important to set out this in sufficient detail, so that the risk can be weighed against the intended benefits.

By using the turnstiles and biometric data for this processing, the school aims to:

1 Comply with safeguarding requirements to ensure information related to keeping children safe is collected and retained appropriately.

2 Manage emergency evacuations in a way that enables an accurate picture of exactly who is on the site at any time of the day, enhancing safety.

3 Provide bespoke reports across the school as required - whether on a pupil, school or whole school level.

4 Provide secure access to staff as required according to their role in the school.

How personal data is processed

This are the who, what, why, how, when, how long for, questions that set out the detail of the personal data to be processed.

Biometric Data

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person. Article 4(14) of the UK GDPR defines biometric data as

""personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm someone's unique identification of that natural person, such as facial images or dactyloscopic data."

Biometric data includes fingerprints. It also includes references or data points taken from these features- even if those points are 'partial' or a full fingerprint could not be reconstructed from the data held. The important thing is that there is something unique about a person's physical or behavioural attributes that is used to identify them.

Additionally, as this biometric data is used to uniquely identify someone, the data is special category data.

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). Information from the individual is compared with biometric information stored in the system to see if there is a match to recognise or identify the individual. To be recognised, an individual must have been previously subject to "enrolment". This is the process where samples of biometric data, such as fingerprints, are captured from an individual and stored to allow comparison in the future.

Use of facial recognition (FR) biometric data for use in cashless catering has attracted the intervention of the Information Commissioner's Office (ICO) with first an advice note for schools and then a reprimand for a school that failed to carry out a DPIA for the use of biometric FR data. In July 2022, the Department for Education updated their non-statutory guidance on the Protection of Biometric Data of Children in Schools and Colleges. The ICO also provide detailed advice on biometric processing on their website. Both of these guidance documents have been taken into account when carrying out this project, and for the completion of this DPIA.

The ievo Data Protection information supplied to the school explains how the system works:

"When registering a fingerprint, the ievo system will scan and extract data using an extraction algorithm which identifies specific features within a fingerprint called minutiae. Identified minutiae points are categorised into groups, which include line bifurcations and ridge endings amongst other data groups. After a registered scan an ievo reader will send an image of the fingerprint to the ievo control board where an advanced algorithm will identify the type, direction and distance between key minutiae features of a fingerprint (Fig 1). This data is converted into a template and stored in a database on the ievo control board. The ***original fingerprint image is not stored or***

recorded[1]*. When using a reader for access a similar process described above will commence. However, this time the matching algorithm will be used to compare the new minutiae data against the stored templates in the database. Once a pre-set number of minutiae points have been matched against a stored template, the user's identity will be confirmed this confirmation will be forwarded to the access control system or 'time and attendance' system for entry and/or data logging…An advanced extraction algorithm is used to create a template from specific fingerprint data captured after a scan. This data (Fig.2) is stored using a unique proprietary template format. All other information is not stored or recorded. The data CANNOT be used to re-construct the original fingerprint image…ievo systems use a cutting-edge Automated Fingerprint Identification System (AFIS) algorithm for data enrolment, extraction and matching processes. This data cannot be reverse engineered to recreate an image of the original fingerprint"*

Fig.1: Image depicting what an ievo reader scans and key minutiae features.

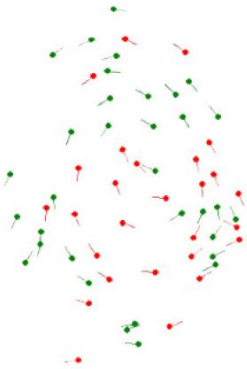

Fig.2: Image depicting key feature data which is extracted, transferred and stored as a template.

Whose personal data will be processed	All pupils in the school (1,700 current pupils). School staff Potentially regular visitors and contractors, or staff from related agencies- such as social services, police, counselling services. depending on the need for them to access and leave the site regularly. However, for most visitors, these individuals will not be part of the biometric system and therefore we will continue to use our [Inventry] system for signing in and out.
What personal data will be processed	Fingerprint data, which will be stored as "key minutiae"- see above for further details.
How will personal data be processed	See above description from ievo setting out how data is processed

[1] The ICO guidance on biometric data says that we should carefully consider the risk of data breach when processing personal data. We consider an important part of our safeguarding of this data to be the fact that fingerprints themselves are not processed. This greatly decreases the likelihood of reverse engineering.

What parties are involved in the processing? What is their role?	The school is controller for the personal data processed by the system. Personal data will remain in the controller of the reader. No data will be held on the reader itself. The controller will be in a secure cabinet on the school grounds. CDVI could remote into the Net2 system but cannot access the controller. Additionally, the system will not have access to the internet and so remote access is not possible. There is no reason for the system to have internet access
Where will personal data be processed and stored?	All processing will take place on a server on the school site, which will only be accessed by the school team.
What due diligence has been completed on the vendor that will be storing and processing personal data?	This is not applicable, as the vendor will not have access to personal data.
Who will have access to the personal data?	Only a limited number of school staff will have access to the personal data. These are the Business Manager, DPO, Operations Manager, Site Manager for processing and managing deletion. In relation to access and security controls, the vendor states: *"ievo systems function with a separate control board which controls an ievo reader, meaning that no information or data is stored locally on reader units themselves. For additional security, the ievo control board, should always be installed on the secure side of an entry point, away from the reader units. ievo readers do not house any locking mechanisms or door relays, meaning that if a reader was removed, your access point would remain secure and your data would remain safe. The reader unit would be deemed useless to the attacker, as it contains no data."*
How long is the data kept for?	Records will be checked on a weekly basis for any staff or student leavers, as well as any written requests that are withdrawing consent, and data will be deleted. At the end of the academic year, all data relating to Years 11 and 13 will be deleted. Should a Year 11 rejoin the sixth form of the school, a new process will begin.

What is the lawful basis for processing?

Identifying the correct lawful basis for processing is an essential part of the DPIA.

Biometric data is a special category of personal data. This means that schools must identify an appropriate lawful basis; in the case of biometric data processed in schools, due to the requirements of the Protection of Freedoms Act 2012, this lawful basis must always be explicit consent. The lawful basis for the school processing this personal data is therefore Article 6(1)(a) consent and Article 9(2)(a) explicit consent.

Consent requirements

When students or staff join the school, a letter regarding the use of biometric data for this purpose is given to them to explain its use, the safeguards in place and to seek explicit consent for the use of their personal data for this purpose. If consent is not given, or withdrawn, then it is possible for the individual to use the turnstile by using a swipe card. We anticipate that only a small number of individuals per year will withhold or withdraw their consent.

Users who use the swipe card will have a dedicated turnstile, which is located in the same area as the main turnstile. We do not anticipate this to lead to any detriment to those individuals; it will be akin to entering a different lane at a toll booth on a motorway where you can choose to pay by cash instead of card. However, we will keep this under review as the project rolls out to ensure that the experience of entering and exiting the site is consistent regardless of whether fingerprint or card is used. We understand that it is important for those who choose not to share this personal data not to experience any detriment.

We understand the ICO guidance around consent for this sort of processing. We understand that as the school, there is a power imbalance between the students and the school, and staff as we are the employer. This means that we understand that we must ensure that people do not receive adverse treatment or feel that cannot refuse consent freely. However, additionally, as a publicly funded organisation, we must ensure that we are not exposed to financial loss as a result of this project- if users continually lose their swipe cards, we could spend excessive amounts of public money on replacing cards. Therefore, whilst the first card will be issued free of charge, we have stated in our consent letter that we will need to charge for lost cards but will replace free of charge faulty cards or when circumstances of the loss are beyond the control of the pass holder.

The consent letters and forms that will be used are included in this DPIA at Annexe 1.

Data subject rights

A summary of how data subjects can exercise their rights should always be considered at the outset of a project. If it is later discovered that it is impossible or difficult for data subject rights to be complied with, this can be difficult or costly to resolve. Rights may differ according to the lawful basis being used.

Data subjects will have appropriate rights over this use of their personal data. In this context, rights related to transparency, erasure and the right to withdraw consent are particularly relevant. We will ensure that the processing is transparent by inclusion of this data processing activity in our privacy notices, and by making information about the nature of the processing very clear when we first seek to obtain consent, not just at the time when we roll out this new project, but also on an ongoing basis as new students and staff join the school. We ensure that all staff are aware of these as well as the other data protection rights and ensure that we adhere to our statutory responsibilities. When individuals withdraw consent or ask for their data to be erased, we will do this without delay (within one calendar month)

Other data subject rights of access, rectification, restriction, and objection will also be upheld- we will seek the advice of our DPO as needed to ensure that the balance between data subject rights and our responsibilities under the law to safeguard children is maintained.

Significance of this processing

It is important to set out the impact of this processing on the affected data subjects. Additionally, it is highly recommended to consider consultation with stakeholders. If consultation is not appropriate, you should be prepared to explain why.

This processing is sensitive and relates to children and staff members' biometric data.

Consultation has been undertaken with students, parents and staff relating to this processing. In early June 2025, the school conducted a consultation exercise with students, staff, and parents to gather views on the proposed biometric site management system. This was carried out via an online survey distributed through the school's communication channels. The survey was sent to 2084 individuals and received 267 (12.81**%)** total responses. Of the 267 responses, 88 people (32.96%) stated they would refuse consent. However, as we would expect those with the strongest of opinions to respond to this survey (people who were unconcerned about the processing may have been less motivated to respond), this does indicate that overall rate of refusal would be more like 4-5%. Therefore, we have calculated that the results indicate broad support (or lack of strong opinion) for the project. The feedback received has been instrumental in shaping the implementation plan, particularly in ensuring that alternative access methods (e.g., swipe cards) are available and that no individual is disadvantaged by choosing not to participate.

Risk assessment

This is a key part of the DPIA process. Having set out the context of the processing, the risk assessment can be carried out. All associated data protection principles and their associated risks are set out, so we can be sure that nothing is accidentally omitted.

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
Lawfulness, fairness and transparency			
We must identify a lawful basis for processing.	The lawful basis for the sharing of data is identified above. Consent/explicit consent is obtained from all individuals before their data is processed. Consent records will be carefully checked before taking any fingerprint data. This is particularly important as children may not feel confident enough to challenge being told that they must line up to give their fingerprint by adults at school. There will be a clear process for the erasure of data where consent is withdrawn.	Very low likelihood of this risk surfacing. In the very rare event that a fingerprint was taken without consent, this would be deleted without delay.	Operations Manager
Processing must be fair.	Processing personal data in schools in this way for the safeguarding of those on site is fair. Whilst it is more intrusive than other forms of ID verification, it forms part of the expected nature of processing in a high security environment, particularly taking into account the concerns raised by Ofsted during their inspection, who expressed that a failproof method of security was required. Fairness is also achieved by ensuring that individuals are not compelled to	Low likelihood of complaints about fairness, as we have built in an alternative method which does not require biometric data to be processed.	Business manager, Operations manager and DPO to keep under review as required, and as part of reviewing this DPIA every 12 months.

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
	participate in this processing- if they do not consent, they will be given a swipe card.		
Data subjects have a right to be informed.	The processing will be transparent if the school ensures that the relevant privacy notices are updated and circulated to include information relating to this processing activity. Individuals also receive additional information as part of the consent gathering process.	Very low likelihood of this risk surfacing.	Privacy notices to be updated and republished on school website before new system goes live. DPO to keep under review as required, and as part of reviewing this DPIA every 12 months.
Data Subjects must be able to exercise their rights under data protection laws.	These rights are already available to data subjects and are explained in the privacy notices- these rights are extended to the data processed for this project. If individuals wish to withdraw consent for this processing, they have the right to do so and this is set out in the consent letter and in the relevant privacy notice. Data can be deleted or retrieved from the system as required to support data subject rights. Any requests for erasure or withdrawal of consent will be processed within one calendar month.	Very low likelihood of this risk surfacing	DPO to keep under review as required, and as part of reviewing this DPIA every 12 months.
Purpose limitation			
Personal data must be collected for specified, explicit and legitimate	The school will not use the personal data for any other purpose beyond what it already does or reasonably needs to in pursuance of	Very low likelihood of this risk surfacing	DPO to keep under review as required, and as part of

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
purposes and not further processed in a manner that is incompatible with those purposes	the aims stated in this DPIA. If any further new processing is intended, then a compatibility assessment and new DPIA will be conducted as required.		reviewing this DPIA every 12 months.
Data adequacy, relevancy and minimisation			
Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The minimum amount of data is processed, and original fingerprints are not retained on the system.	Data already is minimised as the minimum necessary for this processing to take place.	Very low likelihood of this risk surfacing	staff responsible for the data set with supervision of Business Manager and DPO - keep under review as required, and as part of reviewing this DPIA every 12 months.
Accuracy			
The school is responsible for ensuring personal data is accurate. We understand that some degree of error is unavoidable in biometric recognition systems. Our current understanding is	We will monitor the performance of the system to ensure accuracy- including false acceptance and rejection rates, keeping in mind that false acceptance rates could directly lead to a risk as inaccurate data about who is on site will be recorded, and excessive rejection rates will mean that people may lose confidence in the system and it will not	At this time we believe there is a low likelihood and low impact of any accuracy issues surfacing, however, we will keep this under close review.	The Business Manager and Operations Manager will keep this under review as required, and as part of reviewing this DPIA every 12 months.

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
that fingerprints do not change as you grow older, but may be more difficult to read in older adults i.e. much later in life. According to research the ievo ultimate biometric reader delivers a success rate above 99%.	operate as efficiently as intended. We will also monitor rates of acceptance and rejection across different ethnicities to ensure that those who have different skin colours do not experience bias or discrimination.		
Storage limitation			
Personal data should not be processed for longer than required.	The Operations Manager is responsible for ensuring that records are deleted promptly when an individual leaves the school (whether student or staff member) and that this is done at regular intervals every school year	Very low likelihood of this risk surfacing	The Operations Manager, the Data manager and school DPO to review this every summer holiday.
Integrity and confidentiality (security)			
Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or	Ensure all school staff comply with instructions and guidance regarding data protection and IT usage. The school ensures that staff are regularly trained in data protection matters. Cyber-attacks are another high risk to schools- staff are given regular training, guidance and instruction to minimise the risk of cyber-attack. Staff error is the main reason for data breaches the- DPO regularly trains	If all mitigations are in place and carefully followed by all staff, then there **should be a low likelihood** of risks relating to security arising. However, in a large organisation, with such extensive data processing, we are aware that this requires **particular vigilance** to ensure that the likelihood is low. The potential impact of our mitigations failing means that there **could be a high impact** to data subjects, with a	DSL, IT team and DPO to keep under review as required, and as part of reviewing this DPIA every 12 months.

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
organisational measures. The severity of harms caused by biometric data breaches may be greater than with other types of personal information due to its sensitive nature. Biometric data represents key features of a person's physical identity that can't easily be changed. This can result in an indefinite loss of control of personal information if biometric data is not appropriately protected. There is a risk that this processing could result in a data breach.Including examples of risks: -Motivated intruders may try to hack the system to access personal data -Personal data may be accidentally or	staff, and school leadership also regularly remind and support staff to ensure that they process personal data with care and attention.	loss of confidentiality of their data. The impact would depend (if a staff member is given more access than needed is less high impact than a cyber-attack for example).	

Description of risk	Mitigation actions that must be carried out	Risk rating *after mitigations have been carried out*	Person/role responsible and if applicable, date of completion
maliciously deleted.			
Accountability			
All parties have responsibilities to account for their data protection practices. This DPIA and the documents referred/linked to in this document form part of the accountability practices of the school.	Retain evidence of work done to comply with Data Protection laws, including this DPIA, and revisions to it. We will also keep evidence of any issues that arise and how we have dealt with them. Add this new processing activity to the Records of Processing Activity (RoPA) Keep this DPIA under review over time as use of the platform may change in the future.	Very low likelihood of this risk surfacing	DPO to keep under review as required, and as part of reviewing this DPIA every 12 months.

Annex 1

Consent letters:

Consent Forms

Covering Letter