GDPR Policy

School vision and values

At Queensbridge we aim to develop well rounded, confident and responsible individuals who aspire to achieve their full potential. We do this by providing a welcoming, inclusive, safe, and supportive learning environment in which everyone is equal and all achievements are celebrated.

RESPECT
- We are responsible for our actions
- We are empathetic
- We are inclusive

COLLABORATION
- We are able to ask for and give support
- We are articulate
- We are a team

PERSEVERANCE
- We don't give up
- We celebrate our mistakes
- We are ambitious

POSSIBILITIES
- We are globally aware
- We are forward thinking
- We are curious

1. Summary

Sharing information across organisational and professional boundaries can bring many advantages, not least to ensure effective co-ordination, integration of services and multi-agency working.

Information sharing does of course present risks and these need to be managed correctly. It is important to have a clear framework in place which adopts good practice.

The school is committed to sharing information where it is appropriate to do so, whilst ensuring that this is done in a fair and transparent way which is in line with rights and expectations of pupils and their families.

This policy covers all information shared by the school which constitutes personal information as defined by the GDPR. This means any data which relates to a living individual who could be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual.

2. Scope

2.1. This policy covers all of the following, including (but not limited to):

- Pupils and their families
- permanent staff
- temporary staff
- volunteers
- any third parties which may access the school's information assets (including

Hackney Education, suppliers of services, partners)

3. What constitutes Information Sharing?

3.1. Sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;
- different parts of an organisation making data available to each other; or
- exceptional, one-off disclosures of data in unexpected or emergency situations.

4. Statutory Information Sharing

4.1. Key information is shared on a statutory basis and within a defined structure to:

- meet the legal requirement under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013 to share information about our pupils with Hackney Education (HE) and the Department for Education (DfE)
- Make necessary arrangements for school admissions applications
- Support and ensure appropriate provision for pupils with SEND
- To notify HE if a pupil is being removed from the school roll and to notify them within 5 days when a pupil joins the school roll.

4.2. Generally speaking, the data sharing relationship between a school and the local authority is more co-operative than in a standard controller-processor or controller-controller relationship. The care and needs of the learner are critical, and this involves sharing a wide range of information both about the learner themselves and those individuals, such as school personnel, who they come into contact with. It may also involve data sharing among a wider group of organisations than simply the local authority and the school, for example involving health services and the Education Funding Authority.

5. Sharing information with other organisations

5.1. Key information may be shared with Hackney Education (The London Borough of Hackney) or other organisations to:

- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Ensure the safety of pupils whilst in our care and protect children from harm
- Notify families of pupils of any news and important information about the school

- To support integrated health services
- Facilitate commissioning of services to support pupil learning
- Comply with court orders
- Prevent crime or disorder
- Investigate complaints or potential legal claims
- Comply with medical reports / insurance requests
- Provide data for medical, health or social care research (subject to ethical approval)

6. Information Sharing Agreements and Data Processing Agreements

6.1. An Information Sharing Agreement will be used when the school, acting as data controller, is sharing information directly with other organisations that will act either as a joint data controller with the school, or as data controllers in their own right in relation to that information (i.e. a controller-controller relationship) (see **Appendix A**).

6.2. A Data Processing Agreement will be used if a third party organisation is processing personal data on behalf of the school (i.e. a controller-processor relationship). A data processing agreement may take the form of a contract including the data protection clauses and schedule recommended in the HE guidance note titled 'Reviewing arrangements with data processors'.

6.3. The GDPR makes processors responsible for ensuring their data processing is compliant. Processors, as well as controllers, may now be liable to pay damages or be subject to fines or other penalties in the same way as data controllers.

6.3. Depending on the circumstances, the school will have in place either;

- a Data Processing Agreement containing the recommended clauses; or
- an Information Sharing Agreement if the school is sharing personal data with another data controller (see **Appendix A**).

7. Internal sharing of sensitive information for safeguarding purposes

7.1. In order to effectively discharge our statutory responsibility to safeguard and promote the welfare of children and young people, the school understands that the appropriate sharing of sensitive information amongst school staff can be essential.

7.2. In order to control the sharing of sensitive information for safeguarding purposes, and to ensure access to this information is strictly limited to individual staff members who need to see it, the school will use the Safeguarding Information Sharing Protocol attached as **Appendix B**.

8. Roles and Responsibilities

1. The Headteacher and Chair of the Governing Body, in their capacity as representatives of the data controller for the purposes of the GDPR and DPA (2018) will have ultimate decision making power as to whether or not the school shares any personal information.
2. The Data Protection Officer (DPO) will review any proposed information sharing initiatives and agreements in their advisory and monitoring role. It is still the school's responsibility as a data controller to ensure compliance with any relevant legislation, so the DPO will not be held personally responsible if anything goes wrong.
3. The DPO will ensure all information sharing arrangements are formalised through the creation of an Information Sharing Agreement.
4. The DPO will review any ISAs in order to provide independent advice to the Headteacher/Chair of Governing body as required.
5. All parties will adhere to this policy and the **Information Sharing Procedure** when considering sharing personal information.
6. If the information sharing involves any new technologies or serves any new purposes the school will undertake a privacy impact assessment in accordance with the **Privacy Impact Assessment Procedure**.
7. The DPO will provide advice and guidance during the privacy impact assessment.
8. The Headteacher and/or the Chair of the Governing Body will approve the privacy impact assessment, accepting or overriding any DPO advice at their discretion.
9. The DPO will review and update the school's Information Asset Register to reflect any changes in terms of how the school shares any personal information.
10. The DPO will ensure school staff are aware of their responsibilities in relation to information sharing.

9. Review and evaluation

9.1. The Data Protection Officer is responsible for ensuring that this policy remains up to date and accurate. This policy will be reviewed at least annually. Reviews may also take place following:

- any major breaches of a policy
- the identification of new threats or vulnerabilities
- significant organisational restructuring
- significant changes to the school's technical infrastructure

Agreed by governors Autumn 2021.
To be reviewed every two years.

Appendix A: Information Sharing Procedures

Introduction

This procedure underpins the overarching **Information Sharing Policy** and must be followed when entering into an information sharing arrangement.

Information sharing can present risks and these need to be managed correctly. We need to ensure that Information Sharing is carried out fairly and lawfully and in adherence with any and all relevant data protection and privacy legislation.

Step One - Deciding to share personal data

Personal data sharing is not an automatic assumption and there must be a clear purpose for doing so. At this stage you should consider whether you could achieve your goal without sharing any personal data.

Step Two – Consider Anonymisation / Pseudonymisation

Full or partial Anonymisation or Pseudonymisation should be considered ahead of any information sharing arrangement and before deciding to share personal data. The Information Commissioner's Office has published an Anonymisation Code of Practise which is available here. This Code discusses when personal data should be anonymised, the various ways in which data can be anonymised and what constitutes genuine anonymisation. If your objective can be met in a privacy friendly way then personal data should not be shared.

Step Three - Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a process which helps an organisation to identify and thereby reduce the privacy risks when handling personal data.

The following Privacy Impact screening questions must be completed for any new activity relating to personal information to assess whether a full Privacy Impact Assessment is required. The DPO will assess the screening question submission and will advise whether a full PIA is mandatory or recommended and the reasons why.

Privacy Impact Screening Questions:

1. **What is the name of the project or activity this information sharing relates to?**
2. **What is the purpose(s) of the project and why does the personal data need to be shared in order to achieve it?**
3. **What information will be shared?**
4. **Does the project/data processing activity require sharing any special category data?**

5. **Are the purposes described in response to question 2 described or referred to in the Privacy Notice?**
6. **Which individuals or organisations will the personal information be shared with?**
7. **Does the project/data processing activity involve any new systems/technology?**
8. **Does this project/data processing activity involve automated decision making processes (i.e. using algorithms or profiling to make decisions that will affect the individuals to whom the data relates)?**
9. **Does the project/data processing relate to profiling of citizens (e.g. gang membership)?**
10. **Does the project/data processing combine or match personal data from multiple sources?**

Any risks identified as a result of a Privacy Impact Assessment must be mitigated. A decision must be taken by the Headteacher or Chair of Governing Body, having been advised by the DPO, as to whether the risks are acceptable or whether the proposed project/data sharing activity should be cancelled/abandoned.

Step Four – Creation of the Information Sharing Agreement (if required*)

Information sharing between organisations is often dealt with in a tiered approach:

- The ***top tier*** being a shared document defining the commitment to key principles, standards and purposes between organisations (the Protocol).

It is mainly initiated between organisations who regularly and routinely share information for one purpose or another. The signatories are required to meet a stated set of standards and agree to the terms to ensure collaborative working is undertaken in a structured, legal and fair way, which in turn ensures the protection and privacy of personal data. Having already agreed these standards can make further sharing much easier. It further provides individuals (the Data Subjects), with the confidence that we are protecting their information in an appropriate manner.

- The ***middle tier*** being that of the functional agreement, which defines the clear objective, the legal basis to share, details the information to be shared, how it will be shared and when (the Agreement). This is the most common form of ISA required for the sharing of relatively small amounts relatively low risk personal data .

An Information Sharing Agreement (ISA) details the specific arrangements between organisations who need to share information for a common purpose or project. This is the most important of the documents as it provides all parties with clear instructions and information as to how the sharing will work and what the legal restrictions are.
An ISA allows organisations to formalise the decision taken to share and ensure that data protection and privacy requirements have been considered.

- The ***third tier***, (where required) being the tools and methods for actually sharing (day to day procedures).

In larger projects or where sharing involves particularly high volumes or sensitive personal data the ISA will also be backed up by agreed procedures with regards to day to day processing arrangements. These procedures are there to enhance security of the information to both parties. You may feel it is appropriate to create additional procedures alongside your Agreement.

Step Five – ISA approval and sign-off

The DPO may advise on the contents of the ISA but will not provide formal approval.

All information sharing agreements must be sent to the Headteacher or Chair of Governors for oversight and approval.

Whilst it is required to ensure you have an ISA in place ahead of any sharing arrangement it is noted that in one-off, or emergency situations is it not always appropriate to fully draft out and agree an ISA ahead of sharing.

That said this does not remove your data protection obligations around security and privacy. It is important to note that the thought process must still be followed to ensure you have the appropriate legal basis to share the information and information must still be shared in a secure way. E.g. sharing a list of vulnerable pupils during an emergency incident.

Step Six –ISA Register

All approved information sharing agreements must then be stored securely and recorded on Information Asset Register.

ISA Review

A review of the information sharing agreement must take place at regular intervals. Unless there is a justifiable reason for extension, this must be at least annually.
The review must assess the success of the agreement and the procedures followed for appropriate and effective information management sharing and security. Changes in legislation and developments in the areas of public sector data sharing must be taken into account as part of the review as and when they arise.

During the review all elements of the sharing agreement must be addressed and checked for compliance. The aim of the review will be to ensure the scope and purpose are still relevant and the scope has not slipped and the benefits to the data subject are being realised. The review must ensure that the data subjects are still the focus of the sharing arrangement and the arrangement is still benefiting the individuals whose data is being shared.

Termination of Agreements

In the event of an agreement being terminated all parties must agree and put in place appropriate arrangements for the secure return or disposal of the data previously shared.

You must then advise the Information Management Team that the ISA is no longer, confirm what has happened to the data and the ISA will be logged on the register as "expired".

Appendix B: Safeguarding Information Sharing Protocol – Sharing Personal Information Between School Staff

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

In order to effectively discharge our statutory responsibility to safeguard and promote the welfare of children and young people, the school understands that the appropriate sharing of information amongst individual school staff can be essential.

Information will be owned by the Designated Safeguarding Lead who may, on occasion, chose to share this with members of school staff. This decision will be made using common sense and professional judgement. As a guide, the closer the professional is to direct work with the child in question, the more information will need to be shared. This information remains confidential and cannot be shared by the person receiving it without the expressed permission of the DSL.

The following recording form must be attached to the pupil's child in need or child protection

Internal Information Sharing Form
Description of information being shared: insert brief description of the information being shared.
Designated Safeguarding Lead

I am sharing this information with the colleague specified below in order to effectively discharge our statutory responsibility to safeguard and promote the welfare of children and young people in our care. Name (printed): Signature: …….. Dated:
Staff member (recipient)
I receive this information in the knowledge that I am unable to share this further, without the expressed permission of the Designated Safeguarding Lead. I acknowledge that this information is privileged and is shared with me with the intention of ensuring children are protected from harm and that their safety and welfare is promoted. Name (printed): Signature: …… Dated: