Tannery Drift
First School

Enjoyment – Achievement – Respect

Data Protection Policy

Last Review Date:
May 2022

Next Review Date:
May 2023

Artsmark Gold Award
Awarded by Arts Council England

www.tannerydrift.herts.sch.uk

Data Protection Policy

1. Policy Statement and Objectives

1.1 The objectives of this Data Protection Policy are to ensure that Tannery Drift First School and its governors and employees are informed about, and comply with, their obligations under the Data Protection Act 2018 (DPA 2018), UK General Data Protection Regulation (UK GDPR) and with other Data Protection legislation.

1.2 The school is a community school and is the Data Controller for all the Personal Data processed by the school.

1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities, we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4 The type of information that we may be required to handle include details of job applicants, current, past, and prospective employees, pupils, parents / carers and other members of pupils' families, governors, suppliers, and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK GDPR and other legislation. The UK GDPR imposes restrictions on how we may use that information.

1.5 This policy does not form part of any employee's contract of employment, and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the UK GDPR may expose the school to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the school's employees. At the very least, a breach of the UK GDPR could damage our reputation and have serious consequences for the school and for our stakeholders.

2. Status of the Policy

This policy has been approved by the Governing Body of the school. It sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation, and destruction of personal information.

3. Data Protection Officer

3.1 The Data Protection Officer (the 'DPO') is responsible for ensuring the school is compliant with the UK GDPR and with this policy. This post is held by HfL Education, dpo@tannerydrift.herts.sch.uk. In addition, a Data Protection team will be appointed by the school.

Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

3.2 The DPO will play a major role in embedding essential aspects of the UK GDPR into the school's culture, from ensuring the Data Protection principles are respected to preserving Data Subject rights, recording Data Processing activities and ensuring the security of Processing.

3.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, the UK GDPR requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

- senior management support.
- time for DPOs to fulfil their duties.
- adequate financial resources, infrastructure (premises, facilities, and equipment) and staff where appropriate.
- official communication of the designation of the DPO to make known existence and function within the organisation.
- access to other services, such as HR, ICT, and security, who should provide support to the DPO.
- continuous training and sufficient resources to enable the DPO to meet their UK GDPR obligations.
- where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member.
- whether the school should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.4 The DPO is responsible for ensuring that the school's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the school must ensure the independence of the DPO.

3.5 The school will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e., the Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the school's governors are made aware of the pertinent Data Protection issues. In the event that the school decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

3.7 The DPO will operate independently and will not be penalised for performing their task.

3.8 A DPO appointed internally by the school is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with their role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

3.9 In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing Personal Data. However, it should be noted that most of the purposes for processing are either statutory or required to carry out our core activities as a public authority.

3.10 In light of this and in the event that the school decides to appoint an internal DPO, the school will take the following action in order to avoid conflicts of interests:

- identify the positions incompatible with the function of DPO.
- draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate.
- include a more general explanation of conflicts of interests.
- declare that the DPO has no conflict of interests with regard to their function as a DPO, as a way of raising awareness of this requirement.
- include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

3.11 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

4. Definition of Terms

- Biometric Data means Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.
- Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of Personal Data relating to them.
- Data is information, which is stored electronically, or in paper-based filing systems or other media.
- Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

- **Data Controllers** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

- **Data Users** include employees, volunteers, governors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our Data Protection and security policies at all times.

- **Data Processors** means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller.

- **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child.

- **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

- **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

- **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Special Category or Sensitive Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5. Data Protection Principles

Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

- 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 organisational measures.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

6. Processed lawfully, fairly and in a transparent manner

6.1 The UK GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the school), who the Data Controller's representative is (in this case the DPO), the purpose for which the Data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

6.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

- where we have the Consent of the Data Subject.

- where it is necessary for the performance of a Contract.

- where it is necessary for compliance with a legal obligation.

- where processing is necessary to protect the vital interests of the Data Subject or another person.

- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

- where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6.3 Personal Data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the DPA 2018. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the Data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

6.4 Special Category / Sensitive Personal Data

Some of the conditions for processing Special Category (defined in paragraph 4.13) and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the regulations. Appendix 2 of this policy acts as the APD for processing Special Category data.

6.4.1 The school will be processing Special Category/Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Personal Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Special Category/Sensitive Personal Data.

6.4.2 When Special Category/Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 6.2 above), a separate condition for processing it must be met. The additional bases which allow processing of Special Category Personal Data are:

- the Data Subject's explicit consent has been given.
- for employment, social security, and social protection purposes.
- for vital interests.
- for legitimate activities by a foundation, association or any other not for profit body with political, philosophical, or religious or trade union aim.
- for defence of legal claims.
- for substantial public interest purposes.
- for health and social care purposes.
- for public health purposes.
- for archiving, research, and statistics purposes

6.4.3 The school recognises that in addition to Special Category/Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Special Category/Sensitive Personal Data.

6.5 Criminal convictions and offences

- There are separate safeguards in the UK GDPR for Personal Data relating to criminal convictions and offences.
- It is likely that the school will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.
- In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the school in specific circumstances, for example, if a child

protection issue arises or if a parent / carer is involved in a criminal matter.

- Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the Data secure.

6.6 Transparency

One of the key requirements of the UK GDPR relates to transparency. This means that the school must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

One of the ways we provide this information to individuals is through a privacy notice which sets out important information about what we do with their Personal Data. The school has developed privacy notices for the following categories of people:

- Pupils & Parents
- Staff
- Governors

The school wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to the premises or if we ask people to complete forms requiring them to provide their Personal Data.

We will ensure that privacy notices are concise, transparent, intelligible, and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

6.7 Consent

The school must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s). In the event that we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, depending on the circumstances, the school should consider whether it is appropriate to inform Parents about this process. Consent is likely

to be required if, for example, the school wishes to use a photo of a pupil on its website or on social media. Consent is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent if the pupil is aged under 13. When relying on Consent, we will make sure that the child can demonstrate sufficient maturity to understand what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category/Sensitive Personal Data. Often, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Category/Sensitive Data.

Evidence and records of Consent must be maintained so that the school can demonstrate compliance with Consent requirements.

Consent mechanisms must meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7. Specified, explicit and legitimate purposes

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any Data which is not necessary for that purpose should not be collected in the first place.

The school will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

8. Adequate, relevant, and limited to what is necessary

The school will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

In order to ensure compliance with this principle, the school will check records at appropriate intervals for missing, irrelevant, or seemingly excessive information and may contact Data Subjects to verify certain items of Data.

Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a business function, and we should not collect excessive Data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

The school will implement measures to ensure that Personal Data is processed on a 'Need to

Know' basis. This means that the only members of staff or governors who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the school may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Special Category/Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the school's Data Retention guidelines.

9. Accurate and, where necessary, kept up to date

Personal Data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Data should be destroyed.

If a Data Subject informs the school of a change of circumstances their records will be updated as soon as is practicable.

Where a Data Subject challenges the accuracy of their Data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Notwithstanding paragraph 9.3, a Data Subject continues to have rights under the UK GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 9.3 has been followed.

10. Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

Personal Data should not be kept longer than is necessary for the purpose for which it is held. This means that Data should be destroyed or erased from our systems when it is no longer required.

It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete Data is properly erased. The school has a retention schedule for all Data.

11. Data to be processed in a manner that ensures appropriate security of the Personal Data

The school has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they

have suffered damage from such a loss.

We will develop, implement, and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

The UK GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must follow all these procedures and technologies and must comply with all applicable aspects of our Data Security Policy and not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

Maintaining data security means guaranteeing the confidentiality, integrity, and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who are authorised to use the Data can access it.
- Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the Data if they need it for authorised purposes.

It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

Please see our Data Security Policy for details for the arrangements in place to keep Personal Data secure.

Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Governors should be trained on the school's Data Protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

- Ensure that Personal Data which comes into their possession as a result of their duties is kept secure from third parties, including family members and friends.
- Ensure they are provided with a copy of the school's Data Security Policy.
- Using only a school email address (@tannerydrift.herts.sch.uk) or GovernorHub for school related communications.

- Ensuring that any school related communications or information stored or saved on an electronic device or computer is password protected (and encrypted).

- Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties.

Governors will be asked to read and sign an Acceptable Use Agreement.

12. Processing in line with Data Subjects' rights

Data Subjects have rights when it comes to how we handle their Personal Data. Some of these rights may not apply depending on the lawful basis being used for Processing. These include rights to:

- withdraw Consent to Processing at any time.

- receive certain information about the Data Controller's Processing activities.

- request access to their Personal Data that we hold.

- prevent our use of their Personal Data for direct marketing purposes.

- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data.

- restrict Processing in specific circumstances.

- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest.

- request a copy of an agreement under which Personal Data is transferred outside of the EEA.

- object to decisions based solely on Automated Processing, including profiling (Automated Decision Making).

- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

- make a complaint to the supervisory authority (the ICO); and

- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used, and machine-readable format.

We are required to verify the identity of an individual requesting Data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

13. Dealing with Subject Access Requests

The UK GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them may be made in writing or verbally. The school can invite a Data Subject to complete a form, but we may not insist that they do so.

It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the UK GDPR. In some cases, a Data Subject may mistakenly refer to the 'Freedom of Information Act', but this should not prevent the school from responding to the request as being made under the UK GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the UK GDPR and a request for information under the Freedom of Information Act 2000 (FOIA). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is 30 calendar days.

As the time for responding to a request does not stop during the periods when the school is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of Data Subjects to request access to their Data by checking the subject access request email address at regular intervals during periods of holiday closure lasting longer than two weeks.

The school may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

Requests from pupils who are considered mature enough to understand their rights under the UK GDPR will be processed as a Subject Access Request as outlined below and the Data will be given directly to the pupil (subject to any exemptions that apply under the UK GDPR or other legislation). As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own Subject Access Rights. In every case it will be for the school, as Data Controller, to assess whether the child is capable of understanding their rights under the UK GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

Requests from pupils who do not appear to understand the nature of the request will be referred to their Parents or carers.

Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the school considers the child to be mature enough to understand their rights under the UK GDPR, the school shall ask the pupil for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the school to disclose the Personal Data to a Parent without the child's Consent). If Consent is not

given to disclosure, the school shall not disclose the Personal Data if to do so would breach any of the Data Protection principles.

It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the 'Regulations') applies to maintained schools so the rights available to parents in those Regulations to access their child's educational records apply to the school. This means that following receipt of a request from a parent for a copy of their child's educational records, the school must provide a copy within 15 school days, subject to any exemptions or court orders which may apply. The school may charge a fee (not exceeding the cost of supply) for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a Subject Access Request.

Following receipt of a Subject Access Request, and provided that there is sufficient information to process the request, an entry should be made in the school's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of Data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of Data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Where requests are 'manifestly unfounded or excessive', in particular because they are repetitive, the school can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or

- refuse to respond.

However, this will be discussed first with our legal advisors then the Information Commissioner's Office (ICO), as typically they advise organisations to act with a high level of accountability and transparency, which means co-operating with requesters under most circumstances.

Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

In the context of a school a Subject Access Request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

14. Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the school whilst also applying common sense to the circumstances. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

15. Authorised disclosures

The school will only disclose Data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of Personal Data. The school will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Local Authorities
- the Department for Education
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the Teachers' Pension Service
- the Local Government Pension Scheme which is administered by Local Pensions Partnership (LPP)
- our external HR provider, Herts for Learning Ltd trading as HFL Education
- our payroll provider, Hertfordshire County Council
- our external IT Provider
- commissioned providers of local authority services (e.g., Herts for Learning Ltd trading as HFL Education)
- HMRC
- the Police or other law enforcement agencies
- our legal advisors and other consultants
- insurance providers
- occupational health advisors, Optima Health

- the Joint Council for Qualifications
- NHS health professionals including educational psychologists and school nurses
- Education Welfare Officers
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools
- other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances
- confidential waste collection companies

Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be joint controllers of Personal Data and may be jointly liable in the event of any Data Breaches.

Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

The UK GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the Data is Processed ('UK GDPR clauses'). A summary of the UK GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the school to ensure that the UK GDPR clauses have been added to the contract with the Data Processor. Personal Data may only be transferred to a Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

In some cases, Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the UK GDPR, including responsibility for any Personal Data Breaches, onto the school. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

16. Reporting a Personal Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours unless the Data Breach is unlikely to result in a risk to the individuals.

If the breach is likely to result in high risk to affected Data Subjects, the UK GDPR, requires organisations to inform them without undue delay.

It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a

Personal Data Breach to the ICO.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

As the school is closed or has limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects when we develop our Data Breach Response Plan.

If a member of staff, or a governor, knows or suspects that a Personal Data Breach has occurred, our Data Breach Response Plan must be followed. In particular, the DPO or such other person identified in our Security Incident Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

17. Accountability

The school must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with Data Protection principles. The school is responsible for, and must be able to demonstrate, compliance with the Data Protection principles.

The school must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) and an executive team accountable for Data Privacy.
- implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects.
- integrating Data Protection into internal documents including this Data Protection Policy, related policies, and Privacy Notices.
- regularly training employees and governors on the UK GDPR, this Data Protection Policy, related policies, and Data Protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The school must maintain a record of training attendance by all personnel; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. Record keeping

The UK GDPR requires us to keep full and accurate records of all our Data Processing activities.

We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data

Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. Training and audit

We are required to ensure all personnel have undergone adequate training to enable us to comply with Data Privacy laws. We must also regularly test our systems and processes to assess compliance.

Members of staff must attend all mandatory Data Privacy related training.

Data protection awareness training is included in the induction process for all new staff.

20. Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with Data Privacy principles.

This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art.
- the cost of implementation.
- the nature, scope, context, and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

We are also required to conduct DPIAs in respect to high-risk Processing.

The school should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems, or processes), or changing technologies (programs, systems, or processes).
- Automated Processing including profiling and Automated Decision-Making (ADM).
- large scale Processing of Special Category/Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area.

We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children, then a DPIA should be undertaken.

A DPIA must include:

- a description of the Processing, its purposes and the school's legitimate interests if appropriate.
- an assessment of the necessity and proportionality of the Processing in relation to its purpose.
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

21. Walkie Talkies

The school recognises the importance of using Walkie Talkies as a method of communication on the site to ensure that children and staff are kept safe at all times. Reasons for using Walkie Talkies are:

- to summon First-Aid qualified staff in the event of a mishap, and to allow staff on duty outside to summon help if needed.
- to manage behaviour incidents, and to alert staff to attend an incident if required.
- for special events such as Sports Days, school fetes, open days, concerts, school plays, etc.

Staff should be aware that when communicating information over a radio network via a Walkie Talkie, it is possible that anyone in the vicinity who is using the same network may be able to overhear conversations. It is important that appropriate controls are in place to prevent individuals without the correct authorisation intentionally or accidentally gaining access to personal information.

To minimise the risk of unauthorised access to any information that is communicated via Walkie Talkies, staff must ensure that:

- under no circumstances must any personal information be communicated which could enable an individual to be identified e.g., use only first name or initials when referring to named persons.
- the language used during communications is professional, and that no abusive or inappropriate language is used.
- in the event of theft or loss of the equipment, they inform the school's Data Protection team immediately; and
- they have completed and understood the appropriate Data Protection and Security training.

22. Policy Review

It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

This policy should be reviewed by the school periodically and at least every 2 years. It is important to ensure that the DPO is aware of their obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

23. Enquiries

Further information about the school's Data Protection Policy is available from the DPO.

General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Appendix 1

UK GDPR Clauses

The UK GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the UK GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))

2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))

3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)

4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))

5. The Processor must ensure it flows down the UK GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))

6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase, or object to the processing of their Personal Data. (Art. 28(3)(e))

7. The Processor must assist the Data Controller with their security and Data Breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))

8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))

9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under UK law. (Art. 28(3)(g))

10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach UK law. (Art. 28(3))

Appendix 2

Appropriate Policy Document: Special Category and Criminal Offence Data

Summary

This policy outlines the school's obligations under Data Protection Legislation with regard to the processing of Special Category Personal Data and Criminal Offence Data. This should be read alongside our Data Protection policy, our Data Security policy, and our privacy notices.

This document meets the requirements of the Data Protection Act 2018, that an appropriate policy document be in place where the processing of Special Category Personal Data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security, social protection and for reasons of substantial public interest.

The specific conditions under which data may be processed for reasons of substantial public interest are set out in Schedule 1 to the Data Protection Act 2018 and the school intends to rely on these as and when appropriate.

The school will ensure that all Special Category Data is captured, held, and used in compliance with this policy. Any proposed new use of Special Category Data will be subject to a Data Protection Impact Assessment (DPIA). For all uses of Special Category Data, the school will record a description of the lawful basis for processing and confirmation that the appropriate data retention rules are being applied.

Special Category Data

The school is committed to ensuring that all personal data it processes is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The school recognises its duties to protect all personal data but in particular Special Category Personal Data as defined under Data Protection legislation i.e., information that may identify an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Compliance with the Principles of the UK GDPR

Article 5 of the UK GDPR describes 6 principles that we must follow when collecting and using personal information. Where necessary, the school will carry out a DPIA to ensure that processing is compliant with the principles. The following is a summary of our procedures for compliance with those principles regarding Special Category data.

Principle	Procedures for securing compliance
Processed lawfully, fairly and in a transparent manner	The school will: • ensure that such data is only processed where a lawful basis applies. • only process such data fairly and will ensure that data subjects are not misled about the purposes of any processing. • ensure that processing of such data is described clearly in privacy notices available to all data subjects for transparency.
Collected for specified, explicit and legitimate purposes	The school will: • only collect such data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice. • not use such data for purposes that are incompatible with the purposes for which it was collected, and if we do use the data for a new purpose that is compatible, we will inform the data subject first.
Adequate, relevant, and limited to what is necessary	The school will: • only collect and hold such data as necessary for our operational requirements or to meet statutory obligations. • ensure that the data we collect is adequate and relevant.
Accurate and up to date	The school will: • ensure that systems are in place to verify that data is accurate. • ensure that data is kept up to date as necessary.
Kept in a form which permits identification of data subjects for no longer than is necessary	The school will: • ensure data is kept only as long as is necessary for the purposes for which it is collected, or where there is a legal obligation to do so. • where possible, manually delete time-expired data in systems that do not have the functionality to automate disposal.
Processed securely	The school will: • train staff to be particularly aware of the additional risks to Special Category data. • ensure that there appropriate organisational and technical measures in place to protect such data. • take appropriate precautions when transmitting or disposing of the data.

Lawful Bases for Processing

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process Personal Data:

- Article 6(1) (a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
- Article 6(1) (b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- Article 6(1) (c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
- Article 6(1) (d) Vital interests: the processing is necessary to protect someone's life.
- Article 6(1) (e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- Article 6(1) (f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (*This cannot apply to a public authority processing data to perform official tasks, so is generally unlikely to be used*.)

Additional Bases for Processing Special Category Data

The additional bases which allow processing of Special Category Personal Data are:

- Article 9(2) (a) – explicit consent has been given.
- Article 9(2) (b) – for employment, social security, and social protection purposes.
- Article 9(2) (c) – for vital interests.
- Article 9(2) (d) – for legitimate activities by a foundation, association or any other not for profit body with political, philosophical, or religious or trade union aim.
- Article 9(2) (e) – for employment, social security, and social protection purposes.
- Article 9(2) (f) – for defence of legal claims.
- Article 9(2) (g) – for substantial public interest purposes.
- Article 9(2) (h) – for health and social care purposes.
- Article 9(2) (i) – for public health purposes.
- Article 9(2) (j) – for archiving, research, and statistics purposes.

In addition, Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the processing of the special categories of personal data and criminal convictions data. The Schedule is split into four parts:

Part 1 – Conditions relating to employment, health, and research

Part 2 – Substantial public interest conditions

Part 3 – Additional conditions relating to criminal convictions

Part 4 – Appropriate policy document and additional safeguards

In most cases, the Special Category data we collect is covered by Article 6(1) (c) and Article 6(1) (e), along with Article 9(2) (g). In all cases, we will ensure that we record the conditions for processing any type of Special Category data, as defined in both Articles 6 and 9.

Appendix 3

Data Breach Response Plan for Tannery Drift First School

1. Introduction

1.1 Tannery Drift First School has implemented appropriate technical, and organisations measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the school is able to detect it and react swiftly and robustly in order to mitigate any risks to data subjects and to comply with our obligations under the UK General Data Protection Regulation (UK GDPR).

1.2 This Data Breach Response Plan sets out how we will respond to any suspected or actual data breaches and should be read alongside our Data Protection Policy and Data Security Policy.

1.3 The UK GDPR requires the school to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals. In the event that a report is not made within 72 hours, the school is required to provide the reasons for the delay in reporting it to the ICO.

1.4 If there is deemed to be a 'high risk' to the rights and freedoms of individuals following a data breach, the school is also required to notify the individuals affected by the breach. However, in the interests of transparency, the school recognise that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.5 If the school fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this Data Breach Response Plan is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.6 The school will ensure that staff are aware of and are trained on this Data Breach Response Plan to ensure it is effective should a data security incident occur. In particular, the Data Response Team, identified below, must receive training on their roles and responsibilities should a breach occur. For example, our external IT support must be trained on how to identify if the security of our IT systems has been compromised and the steps that need to be taken to respond to a breach, for example, if data on a remote device needs to be wiped. Further details of our security procedures are set out in our Data Security Policy.

1.7 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this Data Breach Response Plan to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

1.8 The school's DPO is HFL Education

2. What is a personal data breach?

The legal definition of a personal data breach is, 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

- Loss or theft of data or equipment.
- People gaining inappropriate access to personal data.
- A deliberate attack on systems.
- Equipment failure.
- Human error.
- Acts of God (for example, fire or flood).
- Malicious acts such as hacking, viruses, or deception.

Examples of common personal data breaches include:

- Sending an email to the wrong recipient.
- Losing a USB stick which contains personal data.
- Having a laptop stolen which contains personal data.
- Sending a letter or email to the wrong address.
- Network, phishing, malware, or other cyber security incidents.

A security incident resulting in personal data being made unavailable for a temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of data subjects, for example, if our IT system goes down. This type of breach should be recorded in the school's Data Breach Log, set out in Appendix 4, so that we keep records of all such incidents. However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a 'breach of security'.

3. Understanding the risk to the rights and freedoms of individuals

A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

When assessing the risk to individuals, the DPO must consider the following factors:

- the type of breach.

- the nature, sensitivity, and volume of personal data.
- ease of identification of individuals.
- severity of consequences for individuals.
- special characteristics of the individual.
- special characteristics of the data controller; and
- the number of affected individuals.

4. Timescales for reporting a breach

The school is required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

It is likely that the school will be deemed as having become 'aware' of a breach when we have a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The UK GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to ensure that we will be 'aware' of any breaches in a timely manner so that we can take appropriate action.

While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected data subjects.

It is possible that we may not have established all of the relevant facts following a data security breach or completed our investigation within 72 hours. However, in the event that the school determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

In the event that we investigate a suspected breach, and we are able to establish that no actual breach has occurred, the Data Breach Log in Appendix 4 must still be completed so that we can keep records of 'near misses' or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

5. Response plan

A member of staff within the school who becomes aware of a suspected or actual data security breach must inform the Headteacher OR the School Business Manager by email

without delay.

If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

The Headteacher or School Business Manager will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If it is decided not to escalate it to the DPO, the Data Breach Log in Appendix 4 must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the DPO. The Data Breach Log should be emailed to the DPO without delay for record keeping purposes.

If the Headteacher or School Business Manager decides to escalate a breach or suspected breach to the DPO, they must do so without delay. Where possible, the Data Breach Log in Appendix 4 must be completed with as much information as possible and emailed to the DPO and copied to the people listed in step 5 paragraph 1. However, if it is not convenient or practicable to complete the Data Breach Log, the report can be made by setting the information out in an email.

Once a breach or suspected breach has been reported to the DPO, the DPO must commence an investigation and assess whether there is sufficient information to identify next steps. The purpose of the investigation is to:

- establish if a breach has happened.
- establish the nature and cause of the breach.
- establish the extent of the damage or harm that results or could result from the breach.
- identify the action required to stop the data security breach from continuing or recurring; and
- mitigate any risk of harm that may continue to result from the breach.

The DPO should contact the Headteacher or School Business Manager if further information is required. The DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

During the course of their investigation, the DPO should consider whether to involve the school's Data Breach Response Team which consists of:

Natalie Phillips, School Business Manager

Helen Gooden, Finance and Administration Officer

Eve Smith Admissions and Administration Assistant

If the DPO is unavailable for any reason, for example, the DPO is on annual leave, on sickness absence or is otherwise not available to respond to the data breach, then the School Business Manager must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan.

If the DPO decides to involve the Data Breach Response Team, the above individuals should be copied into email correspondence and provided with regular updates on the investigation and response to the incident.

The DPO and Data Breach Response Team should take steps to identify any risks arising from the personal data breach:

- Consider obtaining specialist legal advice.
- Confirm the amount, sensitivity, and type of information in question.
- Identify what security measures were in place when the breach occurred as well as what measures have been put in place following it.
- Confirm who has been put at risk and assess the potential harm resulting from the breach.
- Consider the additional consequences of the breach including loss of reputation, loss of business, liability for fines or contractual breaches.

The DPO should consider whether input is required from the school's IT or HR support in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach. As the school has external HR and IT support, the relevant contact details are set out in Appendix 5.

Depending on the circumstances, the DPO should also consider whether the school's insurers should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The DPO should also consider if specialist IT support is required in order to contain and manage a breach and whether the school should engage with local authority PR / media advisors if it is likely that we will need to communicate internally and / or externally with our stakeholders regarding the breach or suspected breach. The contact details for the organisations referred to in this paragraph are set out in Appendix 5.

If the breach or suspected breach has occurred at one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects. It remains the school's responsibility to decide whether to report any such breach to the ICO within 72 hours.

The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller though in this case we need to establish with the joint Data Controller who is going to report the breach to the ICO and the data subjects if such notification is required.

Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the school has fully investigated or contained the breach. A report to the ICO must contain the following information:

- the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned.
- the name and contact details of the DPO or other contact point where more information can be obtained.
- the likely consequences of the personal data breach.
- the measures taken or proposed to be taken by the school to address the personal data

breach, including, where appropriate, measures to mitigate its possible adverse effects.

The DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO should inform the ICO if the school does not yet have all the required information and if further details will be provided later on.

If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the data subjects affected by the breach must also be notified without undue delay. The DPO must liaise with the Headteacher in relation to how the issue should be communicated to the relevant stakeholders. The DPO will need to consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

- description of the nature of the breach.
- the name and contact details of the DPO or other contact point.
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the school to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Given that a large number of our stakeholders are children, if a data breach affects our pupils, it is likely that the above information will need to be given to parents / carers if the affected pupils are aged 12 or under. If the affected pupils are aged 13 or over, the pupils should be informed and it may also be appropriate to notify parents / carers, depending on the circumstances and the nature of the personal data which has been compromised.

If the DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. The school should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

Particular consideration will be given to whether there are any parties that we are legally or contractually obliged to notify (e.g., insurers, regulator).

The DPO must complete the Data Breach Log in Appendix 4 before making the referral to the ICO and keep it under review as and when further information comes to light.

In certain circumstances, where justified, and on the advice of law-enforcement authorities, the

school may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Even if the DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the DPO must still complete the Data Breach Log in Appendix 4 and clearly set out the reasons why the DPO is satisfied that a referral is not required. The DPO must keep the decision under review and be prepared to make a referral to the ICO if any circumstances change or if any information comes to light which means that a referral should be made.

Once the breach has been contained and action taken to stop or mitigate the breach, the DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

As part of the review process, the DPO should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the school response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the UK GDPR and if so, whether the data processor is in breach of contract.

6. School holidays

The school recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the school is closed during school holidays. A breach may still occur during these periods, and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

Staff will be able to email the Headteacher and School Business Manager, and the Admin email address, available on our website, will be monitored at regular intervals by an assigned member of staff, so that the school can be alerted should an incident occur.

The DPO will have the contact details for the Headteacher and School Business Manager so that action can be taken without delay should a breach occur.

The DPO should follow the steps set out above as best as they can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the school is closed due to the school holidays and, depending on the circumstances, advice should be sought from

the ICO on the steps the school should take to mitigate any risks.

7. Review

This Data Breach Response Plan will be kept under review by the DPO and may be revised to reflect good practice or changes to our organisational structure.

Appendix 4

Data Breach Log for Tannery Drift First School

The Data Breach Log must be completed by a suitably trained person following any reports of a security breach or suspected breach involving personal data. Staff must follow the school's Data Breach Response Plan following notification of a breach or suspected breach. In the event you are unsure whether to notify the ICO and the data subjects, you should obtain legal advice without delay as the ICO must be informed about notifiable breaches within 72 hours.

The Data Breach Log is an Excel spreadsheet saved in the school admin area of the server. The log includes the following headings:

Information	Response
Date and time this record was completed	
Name of person completing this record	
General description of the breach	
Name and job title of person who originally reported the breach / suspected breach	
Date and time the breach / suspected breach was reported	
Who was the breach / suspected breach reported to?	
Has the Data Protection Officer been informed?	
Has the Data Breach Response Team been notified?	
What are the details of the breach / suspected breach (include as much detail as possible) NB: An investigation must be undertaken where appropriate	
Who is responsible for the breach i.e., the school as data controller, a joint data controller or a data processor?	
Is the breach ongoing or has it been contained? What steps have been taken to minimise the effects of the breach?	
Is any other information required in order to assess the extent of the breach / the risk to data subjects? If so, specify that information here.	
Whose data has / may have been compromised as a result of the breach / suspected breach?	
Type of data involved in the breach / suspected breach	
Does the breach / potential breach involve Special Category Personal Data or information about criminal offences?	
What is the likely risk to individuals?	
Is there likely to be a high risk to individuals?	
Does the breach need to be reported to the ICO? If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?	

Information	Response
If the breach has already been reported to the ICO, confirm the date and time the report was made, who made the report and whether the report was made within 72 hours.	
If a report has been made to the ICO, what advice or recommended actions have been given? Specify any sanctions that are issued by the ICO following a breach.	
If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review.	
Do the data subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified. If data subjects are not going to be informed, explain the reasons why.	
Does the breach need to be reported to the Police?	
Do any other steps need to be taken e.g., comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.	
Is there likely to be press / media interest as a result of the breach? If so, have the appropriate protocols for handling media enquires been followed?	
Outline the actions that need to be taken in response to the breach / suspected breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an investigation under the school's disciplinary policy is recommended. NB: The information provided in response to this question is likely to be a summary as a more detailed report / audit is likely to be required following a data breach which is notified to the ICO.	

Appendix 5

Contact details for external organisations who may need to be involved if there is a data security breach:

Department / Organisation Name	Contact Details
Hertfordshire County Council	01992 555582
HFL Education Data Management Services	01438 544466 help@sd.hertsforlearning.co.uk
HFL Education – HR Services	01438 544463 hrservices@hfleducation.org