THE VALLEY SCHOOL

DATA PROTECTION POLICY

FEBRUARY 2020 (RESOURCES COMMITTEE)

KEY PRINCIPLES

"Learn to Believe – Learn to Achieve"

"Different for Different"

The school has a set of values and beliefs that uphold the importance of privacy for the individual, whether it be a pupil, a member of staff, a parent or member of the community, and this underpins its commitment to data protection.

KEY LINKS

This policy cross-refers to the following policies:

- Staff discipline and conduct
- ICT Acceptable Use
- General Data Protection Regulations (GDPR) (2018)

KEY PRACTICES AND RESPONSIBILITIES

This policy will ensure that confidential data about all staff, children and families is held securely. It will only be shared when there is a clear, legal requirement to do so or where the individual concerned has given express permission for a defined and agreed purpose.

The Headteacher, other staff and governors will ensure that the school complies with General Data Protection Regulations (2018) by ensuring that anyone processing Personal Data must comply with the enforceable principles of good practice:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The School Business Manager and the Headteacher will report to the Board of Governors in the Summer term of each year, indicating how the school complies with each of the enforceable principles in the General Data Protection Regulations (2018) and governors will arrange to carry out a sample of selected staff to confirm that they understand the legislation.

Appendices:

- 1 Privacy Notice
- 2 CCTV
- 3 Data Breach Response Plan
- 4 Policy Statement
- 5 Policy Objectives

KEY PRINCIPLES

Privacy notice for parents/carers of pupils attending The Valley School

The Valley School collects data and information about parents/carers of our pupils so that we can operate effectively as a school. This privacy notice explains how and why we collect parent/carer data, what we do with it and what rights parents have.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the pupil, with whom the pupil lives or whether the pupil has contact with that parent), and also includes non-parents who have parental responsibility for the pupil, or with whom the pupil lives. It is therefore possible for a pupil to have several "parents" for the purposes of education law. This privacy notice also covers other members of pupils' families who we may process data about from time to time, including, for example, siblings, aunts and uncles and grandparents.

Privacy Notice (How we use parent/carer information)

The Valley School is a maintained community school, and as such acts as a Data Controller and Data Processor

The Valley School is working closely with Lonsdale School, Garston Manor and Colnbrook School, and our Data Protection Officer will be the School Business Manager from Lonsdale School. Please contact the school office on 01438 747274 to be put in contact with our Data Protection Officer.

Why do we collect and use parent/carer information?

We collect and use parent/carer information under the following lawful bases:

a. where we have the consent of the data subject (Article 6 (a));
b. where it is necessary for compliance with a legal obligation (Article 6 (c));
c. where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d));
d. 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 (Article 6 (e)).

Where the personal data we collect about parents/carers is sensitive personal data, we will only process it where:

a. we have explicit consent;

b. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; and / or

c. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Please see our Data Protection Policy for a definition of sensitive personal data.

We use the parent/carer data to support our functions of running a school, in particular:

a. to support pupil learning;

b. to monitor and report on pupil progress;

c. to provide appropriate pastoral care;

d. to assess the quality of our services;

e. to comply with the law regarding data sharing;

f. for the protection and welfare of pupils and others in the school, including our safeguarding / child protection obligations;

g. for the safe and orderly running of the school;

h. to promote the school;

i. to send you communications that may be of interest to you which may include information about school events or activities, news, campaigns, appeals, other fundraising activities;

j. in order to respond to investigations from our regulators or to respond to complaints raised by our stakeholders;

k. in connection with any legal proceedings threatened or commenced against the school.

The categories of parent/carer information that we collect, hold and share include:

a. Personal information (such as name, address, telephone number and email address);

b. Information relating to your identity, marital status, employment status, religion, ethnicity, language, medical conditions, nationality, country of birth and free school meal / pupil premium eligibility / entitlement to certain benefits, information about court orders in place affecting parenting arrangements for pupils);

c. child protection / safeguarding information

d. information about criminal proceedings

From time to time and in certain circumstances, we might also process personal data about parents/carers, some of which might be sensitive personal data, information about criminal proceedings / convictions or information about child protection / safeguarding. This information is not routinely collected about parents/carers and is only likely to be processed by the school in specific circumstances relating to particular pupils, 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.

We collect information about parents/carers before pupils join the school and update it during pupils' time on the roll as and when new information is acquired.

Collecting parent/carer information

Whilst the majority of information about parents/carers provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain parent/carer information to us or if you have a choice in this. Where appropriate, we will ask parents/carers for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to ask your permission to use your information for marketing purposes or to request voluntary contributions. Parents/carers may withdraw consent given in these circumstances at any time.

In addition, the School also uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or investigate other issues. CCTV footage involving parents/carers will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

Storing parent/carer data

A significant amount of personal data is stored electronically, for example, on our database, SIMS. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy which is available from either our Office Manager or School Business Manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer a parent/carer we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Who do we share parent/carer information with?

We routinely share parent/carer information with:

- schools/colleges that pupils attend after leaving us;

From time to time, we may also share parent/carer information other third parties including the following:

- our local authority Hertfordshire County Council;
- a pupil's home local authority (if different);
- the Department for Education (DfE);
- school governors/trustees;
- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists,
- Education Welfare Officers;
- Courts, if ordered to do so;
- the Teaching Regulation Authority;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- our legal advisors;
- our insurance providers/the Risk Protection Arrangement;
- Connexions;
- professionals who are involved on an individual basis with pupils and / or their families

Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

In the event that we share personal data about parents/carers with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Requesting access to your personal data

Under data protection legislation, parents/carers have the right to request access to information about them that we hold by means of a "Subject Access Request". To make a request for your child's personal data, or be given access to your child's educational record, contact Data Protection Officer/Office Manager/School Business Manager although any written request for personal data will be treated as a Subject Access Request.

The legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents/carers to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the our data protection responsibilities.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our Office Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

DATA PROTECTION OFFICER

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO via the school office. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

THE VALLEY SCHOOL

DATA PROTECTION APPENDIX 2 CCTV

FEBRUARY 2020-02 (RESOURCES COMMITTEE)

CCTV Policy

1. Introduction

The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at the school. The system comprises a number of static cameras located around the school site. All cameras can be monitored from the Main Reception.

This Code follows Data Protection Act guidelines.

The CCTV system and data is owned by the school.

2. Objectives of the CCTV system

- To protect the school buildings and assets of the school.
- To increase personal safety and reduce the fear of crime.
- To support the Police in a bid to deter and detect crime.
- To assist in managing the school.

3. CCTV Operating

The CCTV is monitored from the main school office by members of the Senior Leadership Team and Administration Staff.

Access to replay or download footage is restricted to trained members of the Senior Leadership Team.

4. Statement of intent

- The CCTV system will be registered with the Information Commissioner Office under the terms of GDPR and will seek to comply with the requirements both of the Data Protection Act and Commissioner's Code of Practice.
- The school will treat the system and all information, documents and recordings obtained and used, as data which are protected by GDPR.
- The system installed is compliant with the GDPR, Human Rights Act and Regulatory Investigation Powers Act.
- Cameras will be used to monitor activities within the school and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school and its staff, students and visitors.
- Cameras are focussed on school corridor areas.
- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

- Information transferred to CD/DVD (or other appropriate media) will only be used for the investigation of a specific crime or incident. This will be stored securely until the end of any retention period and then destroyed securely.
- Release to the media would only be allowed with the written authority of the police if this was required by them as part of a police investigation.
- Warning signs, as required under GDPR, have been placed at key points in the building.

THE VALLEY SCHOOL

DATA PROTECTION – APPENDIX 3 DATA BREACH RESPONSE

FEBRUARY 2020 (RESOURCES COMMITTEE)

The Valley 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 General Data Protection Regulation ('GDPR').

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.

The procedures set out in this document are particularly important as, prior to the GDPR, there was no obligation on the School to notify the Information Commissioner's Office ('ICO') of data security breaches, although it was good practice to report serious breaches.

The 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.

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.

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.

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 IT support team 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 statement.

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.

The School DPO is Mr Allam, School Business Manager, Lonsdale School who can be contacted on 01438 726999. This is part of a consortium arrangement with Garston Manor, Lonsdale School, Colnbrook School and The Valley School. The School Data Protection Lead is Mrs Frost, School Business Manager.

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.
- Breaches can be categorised according to the following three well-known information security principles:
- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data;
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data;
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

A security incident resulting in personal data being made unavailable for 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 Data Breach Log set out in Appendix A 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'.

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.

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 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 A 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.

Response plan

A member of staff within the school who becomes aware of a suspected or actual data security breach must inform Headteacher or the DPO of the School by email without delay. The email address for contacting the Headteacher is head@thevalley.herts.sch.uk and the DPO is Mr Allam, c/o Lonsdale School. Email accounts should be regularly reviewed. The Headteacher of the School should be copied in to the email to the DPO.

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 will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If the Headteacher decides not to escalate it to the DPO, the Data Breach Log in Appendix A 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 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 A must be completed with as much information as possible and emailed to the DPO. 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 they have 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 and/or member of staff who made the report if further information is required.

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

Corina Foster, Headteacher, head@thevalley.herts.sch.uk,

Paula Frost, School Business Manager (Data Protection Lead), paula.frost@thevallley.herts.sch.uk

Kellie Ransom, Office Manager and PA to the Headteacher,
Kellie.ransom@thevalley.herts.sch.uk

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 Data Protection Lead must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Data Protection Lead must have access to the email account identified above to which data breaches are reported.

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 should consider whether input is required from the IT, HR or other support team 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 IT and HR support, the relevant contact details are set out in Appendix B.

Depending on the circumstances, the DPO should also consider whether the School 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/or the Local Authority. The DPO should also consider if specialist IT support is required in order to contain and manage a breach and whether PR advisors should be engaged 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 B.

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 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 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 notification would ordinarily be to the pupils, however, due to the nature of our school it may also be appropriate to notify parents/carers.

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.

The DPO must complete the Data Breach Log in Appendix A 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 A 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 Schools 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 GDPR and if so, whether the data processor is in breach of contract.

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 or has limited staff available 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:

The DPO and Headteachers email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

The DPO will have the contact details for the Headteacher and our IT support 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 or has limited staff available 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.

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 A – Data Breach Log for The Valley School

This 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 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.

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?	

Information	Response
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?	
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	

Information	Response
Does the breach / potential breach involve sensitive personal data[1] 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?**	
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	

1 Information about an individual's: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation.

Information	Response
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. communication 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?	

Information	Response
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 B – Contact details

Herts for Learning Schools IT –
Herts for Learning Legal Team –
Herts for Learning HR advisory Team –
Serco HR and Payroll –

THE VALLEY SCHOOL

DATA PROTECTION – APPENDIX 4 POLICY STATEMENT

FEBRUARY 2020 (RESOURCES COMMITTEE)

1. Policy statement and objectives

1.1 The objectives of this Data Security Policy are to ensure that The Valley School and its governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other data protection legislation.

1.2 The School is a local authority maintained school and is the Data Controller for all the Personal Data controlled/processed by the School.

1.3 The purpose of this policy is to inform staff about their specific responsibilities in maintaining and improving security standards and data management, through their working practices and day-to-day interaction with the School ICT systems.

1.4 We hold personal data on pupils, staff and others to allow the School to conduct its day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage and potentially damage the reputation of the School, its staff and pupils. Therefore everybody has a shared responsibility to be mindful about data security when they are going about their daily activities and consider how data security risks and threats can be minimised.

1.5 The policy applies to all staff of the School whether temporarily or permanently employed. It also applies to contractors engaged by/working with the School or who have access to information held by the School/Trust.

1.6 The School should ensure all staff are aware of and understand the content of this policy. If any staff member is found to have breached this policy, they could be subject to the Disciplinary and Dismissal Policy & Procedure.

1.7 The policy applies to all locations from which the School systems are accessed by staff including remote use and the use of portable devices.

2. Status of the policy

2.1 This policy has been approved by the Governing Body of the School. It sets out our rules on data security and the legal conditions that must be satisfied in relation to the secure handling, processing, storage, transportation and destruction of personal information.

3. Network/Server Security

3.1 Servers should be physically located in an access-controlled environment. Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third party support where there is a specific job function need for such access.

3.2 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

3.3 Servers should have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification.

3.4 Servers should always be password protected, and locked when not in use.

3.5 Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts.

3.6 IT infrastructure such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel.

3.7 Backup Procedures:

3.7.1 Backup software must be scheduled to run routinely, as required, to capture all data as required.

3.7.2 Backups should be monitored to make sure they are successful.

3.7.3 Backup media must be securely stored in a fireproof container.

3.7.4 Backup media stored off-site must be transported and stored securely.

4. Workstation Security

4.1 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

4.1.1 Restricting physical access to workstations to only authorised personnel.

4.1.2 Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.

4.1.3 Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

4.1.4 Complying with all applicable password policies and procedures.

4.1.5 Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

4.1.6 Ensuring workstations are used for authorised purposes only.

4.1.7 Never installing unauthorised software on workstations.

4.1.8 Storing all confidential information on network servers.

4.1.9 Keeping food and drink away from workstations in order to avoid accidental spills.

4.1.10 Complying with the Anti-Virus policy.

5. Password Security

5.1 Requirements:

5.1.1 All system-level passwords (Administrator, etc.) must be changed on a termly basis, as a minimum.

5.1.2 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

5.1.3 All user-level and system-level passwords must conform to the standards described below.

5.2 Standards - All users should be aware of how to select strong passwords. Strong passwords have the following characteristics:

5.2.1 Contain at least three of the five following character classes: Lower case characters; Upper case characters; Numbers; Punctuation; "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/).

5.2.2 Contain at least eight to fifteen alphanumeric characters.

5.2.3 The password is NOT a word found in a dictionary (English or foreign).

5.2.4 The password is NOT a name or common pattern (e.g. 12345678).

5.2.5 Passwords should be easily remembered. One way to do this is create a password based on a song title or other phrase.

5.3 Protective Measures

5.3.1 Do not share passwords with anyone. All passwords are to be treated as sensitive, confidential information.

5.3.2 Passwords should never be written down, unless securely stored, or stored electronically without encryption.

5.3.3 Do not reveal a password in email, chat, or other electronic communication.

5.3.4 Do not speak about a password in front of others.

5.3.5 Always decline the use of the "Remember Password" feature of applications.

6. Access Control

6.1 Staff should only access systems for which they are authorised. Under the Computer Misuse Act 1990 it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

6.2 All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

6.3 Formal procedures will be used to control access to systems. An authorised manager must request each application for access and access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT of any changes requiring such modification/removal.

6.4 Staff should pay particular attention to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documentation.

6.5 Line managers should ensure that all PC files of continuing interest to the business of the School are transferred to another user before a staff member leaves their employment. It is also good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system administrators of the leaving date. Particular attention needs to be taken when access to personal, commercially sensitive or financial data is involved.

6.6 Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software for the School must comply with the terms of this policy and any access control measures with which they are requested to comply with by School staff.

6.7 Physical security to all office areas should be maintained. Staff should feel confident about challenging strangers without an ID badge.

6.8 Clear Desk Policy:

6.8.1 Staff are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of

each working day and to place them securely into desk drawers and cupboards as appropriate.

6.8.2 Although security measures are in place to ensure only authorised access to office areas, staff members should ensure that documents, particularly of a confidential nature are not left lying around.

7. Security of Portable Equipment and Mobile Devices

7.1 Staff using portable computers/laptops must have appropriate access protection, for example passwords and encryption.

7.2 Devices must not be left unattended in public places or left in unattended vehicles at any time. Staff are also responsible for the security of the hardware and the information it holds at all times on or off School property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly

7.3 Staff should always secure laptops, handheld equipment and any removable media when leaving an office unattended and lock equipment away when leaving the office.

7.4 Staff working from home must ensure appropriate security is in place to protect equipment or information being used by non-School staff. This will include ensuring equipment and information is kept out of sight.

7.5 Staff should ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team.

7.6 Staff must ensure that all school data is stored on the school network, and accessed and worked on via LARA. School data must not kept solely on the laptop and should synchronise all locally stored data with the School network server at the first available opportunity if access to LARA is not available.

7.7 Mobile Computing and Storage Devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or School owned, that may connect to or access the information systems at the School. These devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the IT network. These risks must be mitigated to acceptable levels:

7.7.1 To mitigate these risks LARA should be used at every available opportunity. If this is not possible the following should be adhered to;

7.7.2 Encryption - portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must

use encryption or equally strong measures to protect the data while it is being stored.

7.7.3 Database or portions thereof, which reside on the network shall not be downloaded to mobile computing or storage devices.

7.7.4 Report lost or stolen mobile computing and storage devices immediately to the IT department and/or the DPO.

7.7.5 Non-departmental owned device that may connect to the School network must first be approved by the Assistant Headteacher with responsibility for ICT.

8. Acceptable Use

8.1 While the School network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the School.

8.2 Staff must pay particular attention to the protection of personal data and commercially sensitive data. All sensitive files must be password protected or encrypted where possible.

8.3 For security and network maintenance purposes, authorised individuals within the School may monitor equipment, systems and network traffic at any time.

8.4 Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If staff are in doubt as to whether the individual requesting such access is authorised to do so, they should ask for their identification badge and contact their department. Any authorised staff member will be happy to comply with this request.

8.5 Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of the ICT systems; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

8.6 Authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

8.7 All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2018 (RIPA) and the Lawful Business Practice Regulations 2000.

8.8 Please note that personal communications using School ICT systems may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

8.9 Staff must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

8.10 If it is suspected that there may be a virus on any School ICT equipment, staff should stop using the equipment and contact the IT team immediately. They will advise what actions to take and be responsible for advising others that need to know.

8.11 It is imperative that staff do not access, load, store, post or send from School ICT system any material that is, or may be considered to be: illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the School into disrepute. This includes, but is not limited to: jokes, chain letters, files, emails, clips or images that are not part of the School business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

8.12 Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act or a Subject Access Request.

8.13 Where necessary, permission should be obtained from the owner or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

9. Printing, Copying and Transmission of Data

9.1 It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

9.2 Staff should ensure that the entire document has copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.

9.3 Staff should not leave the printer unattended when using it, as another person may pick up the printing by mistake.

9.4 When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All staff should consider the risk of harm or distress that could be caused to the relevant data subject if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

9.5 Send only the minimum amount of personal or sensitive information, by whichever method is chosen.

9.6 Sending information by email:

9.6.1 Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.

9.6.2 If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list.

9.6.3 Take care when replying 'to all' – do they really all need to receive the information being sent.

9.6.4 If emailing sensitive information, password protect any attachments. Use a separate email or different method to communicate the password e.g. telephone call.

9.6.5 When sending sensitive files, consider the use of secure file transfer systems where available, such as Schoolsfx or HertsFX.

9.7 Sending information by post:

9.7.1 Check that the address is correct.

9.7.2 Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.

9.7.3 Consider using tracking, e.g. recorded delivery or a courier if appropriate.

10. Use of Email

10.1 The School gives all staff their own email account to use for all School business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed. GovernorHub is used by all Governors to exchange information and for all communication, except in the case of routine housekeeping (e.g. checking times, letting someone know you are running late etc).

10.2 Staff should use their school email for all professional communication. Communication between staff and Governors must be via the Headteacher, the Headteacher's PA or via the Clerk to the Governors, who will have a school email address only.

10.3 Monitoring – School employees shall have no expectation of privacy in anything they store, send or receive on the School email system. The School may monitor messages without prior notice.

10.4 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

10.5 Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

10.6 All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

10.7 Staff should avoid sending or forwarding attachments unnecessarily. Whenever possible, the location path to the file on a shared drive should be sent instead.

10.8 Staff sending emails to external organisations, parents or pupils are advised to copy in, or blind copy in, the Headteacher or line manager.

10.9 When emailing confidential/personal data, obtain express consent from the Headteacher or line manager to provide the information by email and exercise caution when sending by performing the following checks:

10.9.1 Encrypt and/or password protect attachments. Provide the encryption key or password by a separate contact with the recipient(s).

10.9.2 Verify the details, including accurate email address, of any intended recipient of the information. Do not copy or forward the email to any more recipients than is absolutely necessary.

10.9.3 Verify the details of a requestor before responding to email requests for information.

10.9.4 Consider using other secure file transfer methods, such as HertsFX or Schoolsfx.

10.9.5 Request confirmation of safe receipt.

10.10 The School email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any School employee should report the matter immediately. The following activities are strictly prohibited, with no exceptions:

10.10.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

10.10.2 Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.

10.10.3 Creating or forwarding "chain letters", "joke" emails, or "pyramid" schemes of any type.

10.11 Users should actively manage their email account by:

10.11.1 Checking emails regularly.

10.11.2 Deleting all emails of short-term value.

10.11.3 Organising email into folders and carrying out frequent house-keeping on all folders and archives.

10.11.4 Activating an out-of-office notification when away for extended periods.

10.12 Personal Use - using a reasonable amount of School resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

10.13 The School email account should not be used for personal advertising.

10.14 All the above apply whether accessing the School email account onsite, or through webmail or on non-School devices.

11. Data Breaches

11.1 The Information Commissioner's Office (ICO) has the power to serve notices requiring organisations to pay up to €20 million or 4% of annual global turnover, whichever is higher, for serious breaches of the GDPR and Data Protection Act 2018.

11.2 Staff are responsible for:

11.2.1 Ensuring that no breaches of information security result from their actions.

11.2.2 Reporting any breach, or suspected breach of security without delay.

11.2.3 Ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

11.2.4 Ensuring they are aware of and comply with any restrictions specific to their role or service area. All staff should be aware of the confidentiality clauses in their contract of employment.

11.3 Advice and guidance on information security can be provided by the School DPO or Data Protection Lead.

11.4 A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

11.5 For staff any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

11.6 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, then the actions in the Data Breach Response Plan must be followed. In particular, the DPO or such other person identified in the Data Breach Response Plan must be notified immediately.

11.7 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

12. Disposal of Redundant ICT Equipment Policy

12.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

12.2 All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen.

12.3 Disposal of any ICT equipment will conform to: the Waste Electrical and Electronic Equipment Regulations 2018, the Data Protection Act 2018, the Electricity at Work Regulations 1989.

12.4 The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

12.4.1 Date item disposed of.

12.4.2 Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media.

12.4.3 How it was disposed of e.g. waste, gift, sale.

12.4.4 Name of person and/or organisation who received the disposed item.

12.5 Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

13. Policy Review

13.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis, and at least every 2 years or if any new technologies are introduced. Recommendations for any amendments should be reported to the DPO.

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

14. Enquiries

14.1 Further information can be found in the Acceptable Use of ICT policy and the Data Protection Policy.

Document Control

Date modified	Description of modification	Modified by

14.2 The objectives of the Data Protection Policy are to ensure that The Valley School (the "School") and its governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other Data Protection legislation.

14.3 The School is a local authority maintained school and is the Data Controller for all the Personal Data processed by the School.

14.4 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.

14.5 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 GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

14.6 The policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of the 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 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 GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

15. Status of the policy

15.1 The 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.

16. Data Protection Officer

16.1 The Data Protection Officer (the "DPO") is responsible for ensuring the School is compliant with the GDPR and with the policy. The post is held by the School Business Manager of Lonsdale School as part of a consortium arrangement which

includes The Valley School, Garston Manor School, Lonsdale School and Colnbrook School. The School based Data Protection Lead is the School Business Manager who acts as DPO for a consortium school. Any questions or concerns about the operation of the policy should be referred in the first instance to the DPO.

16.2 The DPO will play a major role in embedding essential aspects of the 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.

16.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do the, the 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:

16.3.1 senior management support;

16.3.2 time for DPOs to fulfil their duties;

16.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

16.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;

16.3.5 access to other services, such as HR, IT and security, who should provide support to the DPO;

16.3.6 continuous training so that DPOs can stay up to date with regard to Data Protection developments;

16.3.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;

16.3.8 whether the School should give the DPO access to external legal advice to advise the DPO on their responsibilities under the Data Protection Policy.

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

16.5 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.

16.6 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.

16.7 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 his or her 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.

16.8 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. Senior management positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

16.9 In the light of the 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:

16.9.1 identify the positions incompatible with the function of DPO;

16.9.2 draw up internal rules to the 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;

16.9.3 include a more general explanation of conflicts of interests;

16.9.4 declare that the DPO has no conflict of interests with regard to his or her function as a DPO, as a way of raising awareness of the requirement;

16.9.5 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.

16.10 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.

17. Definition of terms

17.1 **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;

17.2 **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

17.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

17.4 **Data Subjects** for the purpose of the 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.

17.5 **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.

17.6 **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;

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

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

17.9 **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;

17.10 **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;

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

17.12 **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;

17.13 **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.

18. Data protection principles

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

18.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

18.1.2 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;

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

18.1.4 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;

18.1.5 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 GDPR in order to safeguard the rights and freedoms of individuals; and

18.1.6 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.

19. Processed lawfully, fairly and in a transparent manner

19.1 The 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 the case the School), who the Data Controller's representative is (in the 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.

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

19.2.1.1 where we have the Consent of the Data Subject;

19.2.1.2 where it is necessary for compliance with a legal obligation;

19.2.1.3 where processing is necessary to protect the vital interests of the Data Subject or another person;

19.2.1.4 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.

19.3 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 Act. The 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.

19.4 Sensitive Personal Data

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

19.4.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 19.2 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

19.4.2.1 the Data Subject's explicit consent to the processing of such Data has been obtained

19.4.2.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to Data Protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

19.4.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

19.4.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

19.4.3 The School recognises that in addition to 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 Sensitive Personal Data.

19.5 Biometric Data

The School does not currently use Biometric Data. Should the school move to an automated biometric recognition system, appropriate consultation will take place and the following will be adhered.

19.5.1 The School may process Biometric Data as part of an automated biometric recognition system, for example, for cashless catering or photo ID card systems where a pupil's photo is scanned automatically to provide him or her with services. Biometric Data is a type of Sensitive Personal Data.

19.5.2 Where Biometric Data relating to pupils is processed, the School must ensure that each parent of a child is notified of the school's intention to use the child's Biometric Data and obtain the written consent of at least one parent before the Data is taken from the pupil and used as part of an automated biometric recognition system. The School must not process the Biometric Data if a pupil under 18 years of age where:

19.5.2.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

19.5.2.2 no Parent has Consented in writing to the processing; or

19.5.2.3 a Parent has objected in writing to such processing, even if another Parent has given written Consent.

19.5.3 The School must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. The School will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

19.5.4 The School must obtain the explicit Consent of staff, governors, or other Data Subjects before processing their Biometric Data.

19.6 Criminal convictions and offences

19.6.1 There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

19.6.2 It is likely that the School will Process Data about criminal convictions or offences. The 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.

19.6.3 In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. The 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.

19.6.4 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.

19.7 Transparency

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

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

19.7.2.1 Pupils

19.7.2.2 Parents

19.7.2.3 Staff

19.7.2.4 Governors

19.7.3 The School wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. The means that the privacy notice is just one of the tools we will use to communicate the 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 School premises or if we ask people to complete forms requiring them to provide their Personal Data.

19.7.4 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.

19.8 Consent

19.8.1 The School must only process Personal Data on the basis of one or more of the lawful bases set out in the 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.

19.8.2 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.

19.8.1 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) or legal guardian(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 will inform Parents about the process and consider whether it is appropriate to require their Consent. 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 understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

19.8.2 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.

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

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

20. Specified, explicit and legitimate purposes

20.1 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.

20.2 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.

21. Adequate, relevant and limited to what is necessary

21.1 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.

21.2 In order to ensure compliance with the 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.

21.3 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.

21.4 The School will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. The 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, the 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 Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

21.5 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.

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

22.1 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.

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

22.3 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 the proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at the 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.

22.4 Notwithstanding paragraph 22.3, a Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 22.3 has been followed.

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

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

23.2 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.

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

24.1 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.

24.2 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.

24.3 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.

24.4 The 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 GDPR and relevant standards to protect Personal Data.

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

24.5.1 **Confidentiality** means that only people who are authorised to use the Data can access it.

24.5.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

24.5.3 **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes.

24.6 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.

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

24.8 Governors

24.8.1 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. The includes:

24.8.1.1 Ensure that Personal Data which comes into their possession as a result of their School duties is kept secure from third parties, including family members and friends.

24.8.1.2 Ensure they are provided with a copy of the School's Data Security Policy.

24.8.1.3 Using a School email account for any School-related communications.

24.8.1.4 Ensuring that any School-related communications or information stored or saved on an electronic device or computer is password protected and if possible encrypted.

24.8.1.5 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.

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

25. Processing in line with Data Subjects' rights

25.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

25.1.1 withdraw Consent to Processing at any time;

25.1.2 receive certain information about the Data Controller's Processing activities;

25.1.3 request access to their Personal Data that we hold;

25.1.4 prevent our use of their Personal Data for direct marketing purposes;

25.1.5 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;

25.1.6 restrict Processing in specific circumstances;

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

25.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

25.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);

25.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

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

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

25.1.13 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.

25.2 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.

26. Dealing with Subject Access Requests

26.1 The 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 must be made in writing.

26.2 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 the phrase in their request or refer to the 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 GDPR, if appropriate. Some

requests may contain a combination of a Subject Access Request for Personal Data under the 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.

26.3 Any member of staff who receives a written request of the nature must immediately forward it to the DPO as the statutory time limit for responding is **one calendar month**.

26.4 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 the may have on the rights of Data Subjects to request access to their Data by implementing the following measures:

- School admin email addressed checked during any holiday periods
- A member of the SLT 'on duty' and checking postal communication during holiday periods

26.5 A fee may no longer be charged to the individual for provision of the information (previously a fee of £10 could be charged under the DPA 1998).

26.6 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.

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

26.8 Requests from pupils who are considered mature enough to understand their rights under the 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 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 the 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 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.

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

26.10 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 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.

26.11 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. The 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 for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. The 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.

26.12 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 date on which sufficient information has been provided.

26.13 Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the School can:

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

26.13.2 refuse to respond.

26.14 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.

26.15 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, the 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.

26.16 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.

27. Providing information over the telephone

27.1 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 particular circumstances. In particular they should:

27.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

27.1.2 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.

27.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

28. Authorised disclosures

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

28.2 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:

28.2.1 Local Authorities

28.2.2 the Department for Education

28.2.3 the Disclosure and Barring Service

28.2.4 the Teaching Regulation Agency

28.2.5 the Teachers' Pension Service

28.2.6 the Local Government Pension Scheme which is administered by LGPS

28.2.7 our external HR and payroll provider Serco

28.2.8 our external IT Provider Herts for Learning

28.2.9 HMRC

28.2.10 the Police or other law enforcement agencies

28.2.11 our legal advisors and other consultants

28.2.12 insurance providers

28.2.13 occupational health advisors

28.2.14 exam boards

28.2.15 the Joint Council for Qualifications

28.2.16 NHS health professionals including educational psychologists and school nurses

28.2.17 Education Welfare Officers

28.2.18 Courts, if ordered to do so

28.2.19 Prevent teams in accordance with the Prevent Duty on schools

28.2.20 other schools and colleges, for example, if we are negotiating a managed move or transition arrangements and we have Consent to share information in these circumstances;

28.2.21 confidential waste collection companies;

28.2.22 Connexions

28.3 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.

28.4 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.

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

28.6 The 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 ("GDPR clauses"). A summary of the 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 GDPR clauses have been added to the contract with the Data Processor. Personal Data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

28.7 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 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.

29. Reporting a Personal Data Breach

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

29.2 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.

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

29.4 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

29.5 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.

29.6 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 the may have on Data Subjects when we develop our Data Breach Response Plan.

29.7 If a member of staff or 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.

30. Accountability

30.1 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.

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

30.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for Data Privacy;

30.2.2 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;

30.2.3 integrating Data Protection into internal documents including the Data Protection Policy, related policies and Privacy Notices;

30.2.4 regularly training employees and governors on the GDPR, the 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 School personnel; and

30.2.5 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.

31. Record keeping

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

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

31.3 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.

32. Training and audit

32.1 We are required to ensure all School 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.

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

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

33.1 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.

33.2 The 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:

33.2.1 the state of the art;

33.2.2 the cost of implementation;

33.2.3 the nature, scope, context and purposes of Processing; and

33.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

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

33.4 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:

33.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

33.4.2 Automated Processing including profiling and Automated Decision-Making (ADM);

33.4.3 large scale Processing of Sensitive Data; and

33.4.4 large scale, systematic monitoring of a publicly accessible area.

33.5 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.

33.6 A DPIA must include:

33.6.1 a description of the Processing, its purposes and the School's legitimate interests if appropriate;

33.6.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

33.6.3 an assessment of the risk to individuals; and

33.6.4 the risk mitigation measures in place and demonstration of compliance.

34. CCTV

34.1 The School uses CCTV in locations around the School site. The is to:

34.1.1 protect the School buildings and their assets;

34.1.2 increase personal safety and reduce the fear of crime;

34.1.3 support the Police in a bid to deter and detect crime;

34.1.4 assist in identifying, apprehending and prosecuting offenders;

34.1.5 provide evidence for the School to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other

visitors on the site which breaches or is alleged to breach the School's policies;

34.1.6 protect members of the school community, public and private property; and

34.1.7 assist in managing the School.

34.2 Please refer to the School's CCTV policy/code of practice for more information.

35. Policy Review

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

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

35.3 The 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 his or her obligations under the policy and that they receive the training and other support they need in order to fulfil the role.

36. Enquiries

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

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

Document Control

Date modified	Description of modification	Modified by

Appendix 1 – GDPR Clauses

The GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the 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 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 Union or Member State 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 Union or Member State law. (Art. 28(3))**