Data Security Policy

	Name of school	**Oak Lodge School (including Deaf First)**
	Policy review date	**1 October 2018**
	Date of next review	**1 October 2019**
	Who reviewed this policy?	**Karen Chapman (SBM)**

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Gary Hipple, Head of School ICT / Schools Data protection Officer, is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in an Excel Spreadsheet.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record in SIMS.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.

  - staff
  - governors
  - pupils
  - parents
  - volunteers

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks. We also have an additional layer of monitoring software across our network system. We monitor school e-mails and twitter feeds to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails and twitter feeds.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.

- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, USO admin site, every 90 days.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.School staff who set up usernames and passwords for e-mail, network access, work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources.
- LGfL staffmail for all school related email.
- We use Egress to transfer documents to schools in London, such as references, reports of children.
- We store any sensitive/special category written material in <lockable storage cabinets in a lockable storage area>.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up hard drives in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross-cut shredder or the secure waste bin which is collected and disposed of using secure procedures.

  - Appendix 1 - Subject Access Request Procedure
  - Appendix 2 - Data Breach Procedure
  - Appendix 3 – Data Protection Breach Record
  - Appendix 4 – Schools Data Protection Officer Service Level Agreement
  - Appendix 5 – Data Protection Impact Assessment (DPIA) Records

Oak Lodge School Subject Access Request Procedure

Scope

All personal data processed by *Oak Lodge School* or on behalf of *Oak Lodge School* is within the scope of this procedure.

Data subjects are entitled to obtain:

- Confirmation as to whether Oak Lodge School is processing any personal data about that individual;
- Access to their personal data;
- Any related information;

Procedure

Subject Access Requests (SARs) for information must be made in writing and sent to Karen Chapman School Business Manager. The school will provide a template for the request (appendix 1).

If an individual is unable to provide a request in writing and justifiable assistance is required, it must be provided and the request can be made on behalf of the individual.

Oak Lodge School does not need to respond to a request made orally but, depending on the circumstances, it might be reasonable to do so (as long as Oak Lodge School is satisfied about the person's identity). It is good practice at least to explain to the individual how to make a valid request, rather than ignoring them.

If a request does not mention the Data Protection Legislation specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own or child's personal data.

Requesters do not have to tell Oak Lodge School their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.

A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure you recognise a subject access request (SAR) and forward it to the named person in school who will liaise with the school Data Protection Officer.

Any school employee who receives a request for a subject access request (SAR) must forward it immediately to Karen Chapman School Business Manager, no matter what form it is received in. Karen Chapman School Business Manager will log and acknowledge the request.

The data subject will provide the school with evidence of their identity and the signature on the identity must be cross-checked.
List of acceptable identity includes:

- Passport
- Driving licence
- Birth certificate
- Utility bill (from last 3 months)
- Current vehicle registration document
- Bank statement (from last 3 months)
- Rent book (from last 3 months)

- Council tax

The data subject may specify to Oak Lodge School a specific set of data held by Oak Lodge School on their subject access request (SAR). The data subject can request all data held on them.

Karen Chapman School Business Manager will update the log and record the date that the identification checks were conducted and the specification of the data sought.

Karen Chapman School Business Manager will work with the school Data Protection Officer to provide the requested information to the data subject within one month from this recorded date.

Under the GDPR Article 12 (3), the month deadline may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The [named person/post in school] shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.
Example of reason for the delay:

- Volume of information is over 1,000 pages
- Open complex cases
- Three or more third parties are included

Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Once received, the subject access request (SAR) is immediately forwarded to Karen Chapman School Business Manager, who will ensure that the requested data is collected within the specified time frame.
Collection entails:

- Collecting the data specified by the data subject,
- Request Oak Lodge School to search and retrieve information from all relevant databases and all relevant filing systems (manual files) in the school, including all back up and archived files (computerised or manual) and all email folders and archives.

The Data Protection Officer will maintain a record of requests for data and of its receipt, including dates and copies of correspondences.

All documents should be reviewed that have been provided, to identify whether any third parties are present in it, and either remove the identifying third party information from the documentation or obtain written consent from the third party for their identity to be revealed.

The DPA currently sets out a number of exemptions which allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed. Current exemptions which are relevant include:

- Confidential references – schools do not have to provide subject access to references they have confidentially given in relation to an employee’s employment;
- Management information – personal data which relates to management forecasting or planning is exempt from subject access (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation);
- Legal advice and proceedings – schools do not have to disclose data which is covered by legal professional privilege;
- Settlement negotiations – the subject is not entitled to personal data which consists of a record of the employers intentions in respect of settlement

discussions that have taken place or are in the process of taking place with that individual.

In the event that a data subject requests details of what personal data is being processed then they should be provided with the following information:

- Purpose of the processing
- Categories of personal data
- Recipient(s) of the information, including recipients in third countries or international organisations
- How long the personal data will be stored
- The data subject’s right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
- Oak Lodge School takes appropriate measures to act without undue delay in the event that the data subject has: withdrawn consent (objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

Inform the data subject of their right to lodge a complaint with the ICO and a method to do so.

Inform the data subject of any automated decision-making.

If and where personal data has been transferred and information on any safeguards in place.

Oak Lodge School does not charge a fee for Subject Access Requests (SARs).

Complaints against Subject Access Requests (SARs)

Individuals that wish to make a complaint about the handling of their Subject Access Request (SAR) can raise a concern with the Data Protection Officer. They also have a right to raise their concern with the Information Commissioner’s Office. Any Subject Access Request (SAR) concern received by a school employee must be forwarded to the Data Protection Officer immediately.

Oak Lodge School Form for submitting subject access requests

101 Nightingale Lane, London, SW12 8NA

[Insert date]

Re: subject access request

Dear *school name:*

Please provide me with the information about me that I am entitled to under the Data Protection Act 2018 and General Data Protection Regulation (GDPR). This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Name

Oak Lodge School Data Breach Procedure

Policy Statement

Oak Lodge School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Oak Lodge School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Oak Lodge School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;

- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher or the School Business Manager and the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. The use of back-ups to restore lost/damaged/stolen data.

c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;

- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Data Breach Report Form

Please complete sections 1-4 of the form below to notify the GDPR Team of a suspected data breach. Your completed form should be emailed to Karen Chapman, School Business Manager who will pass it to the DPO, Gary Hipple.

	Report prepared by: **Date:** **On behalf of:**	
1	**Summary of the event and circumstances:**	
2	**Type and amount of data (personal/staff, student, parental/carer):**	
3	**Actions taken to retrieve the information and minimise the effect of the breach:**	
4	**Details of notification to affected data subject:** **(if applicable)** **Has a complaint been received from the affected data subject?**	

Sections 5-8 to be completed in consultation with a member of the Data Protection team.

5	**Breach of procedure / policy by staff member:**	
6	**Details of Data Protection training provided/taken:**	
7	**Any procedure changes required to reduce risks of future data loss:**	
8	**Conclusion:**	

Schools Data Protection Officer Service Level Agreement

Contact

Gary Hipple
ghipple@wandsworth.gov.uk

Purpose

From 25th of May 2018 The General Data Protection Regulation (GDPR) and Data Protection Act 2018 were written in to law. The GDPR is a law designed to protect the privacy of individuals, in particular with regards to the processing of their personal information.

The GDPR requires that all Public Authorities appoint a Data Protection Officer. Schools are defined as Public Authorities. Article 37 (2) of the GDPR allows a group of undertakings to appoint a single data protection officer.

This SLA gives schools the opportunity to fulfil their obligation to appoint a Data Protection Officer in a cost effective way by sharing a central resource, the Wandsworth School's Data Protection Officer service. The GDPR requires the DPO to have professional experience and knowledge of data protection law. This SLA will provide your school with a DPO and assist you with your obligations under the GDPR.

Under the GDPR the school remains the Data Controller and compliance with Data Protection Legislation is ultimately the schools responsibility. The Data Protection Officer's role is to direct, advise and assist.

Changes to the Service Level Agreement

This Service Level Agreement shall be reviewed annually. The services detailed in this Data Protection Officer SLA are available to the schools who subscribe on the condition that enough schools subscribe to wholly fund the service.

Exceptional demands on the service will be prioritised by the Head of Schools ICT.

Data Protection Officer service responsibilities:

The data protection officer service will, in as timely a manner as possible:

- Provide advice to help schools be compliant with the GDPR and Data Protection Act 2018.
- Provide the tools and guidance to complete and update data audit records required for your school
- Provide advice and guidance to schools in relation to Breaches, Issues or Concerns
- Provide Data Protection related policies, procedures and templates.
- Provide Schools with appropriate advice, guidance and recommendations via telephone, email and face to face
- Provide training for staff and governors
- Provide advice and guidance on Information Sharing and assist with completion of all relevant paperwork such as Data Protection Impact Assessments and agreements
- Have their contact details made available on school privacy notices
- Be in a position to undertake their tasks independently – report to highest level of management directly
- Co-operate with the supervisory authority (Information Commissioner's Office)
- Act as contact point for the supervisory authority (Information Commissioner's Office)

- Have due regard to the risks associated with processing, taking account of nature, scope and context of processing
- Promote a data protection culture within the school
- Provide guidance in analysing and checking compliance of processing activities

Schools Responsibilities

Schools will:

- Contact the Data Protection Officer service via email or telephone when a breach is identified and they require assistance
- Notify the Data Protection Officer service in advance of events or requirements that might require a higher than normal level of support
- Provide responses to the Data Protection Officer service in a timely manner. Delays in response may result in requests being delayed
- Advise the Data Protection Officer service when planning a new system installation/plans to share data with third parties
- Advise the Data Protection Officer service in advance of any new projects that could impact on the service, advice and guidance we provide
- Make a request for new service by emailing schoolsdpo@wandsworth.gov.uk

Service Level Agreement Charges

The charges for this service are as set out below.

Nursery & Special schools	£850
Primary Schools 150 – 250 pupils	£950
Primary Schools 251 – 480 pupils	£1100
Primary Schools 481+ pupils	£1250
Secondary schools	£1400

Appendix A

Call Logging – Incident Priorities

The Data Protection Officer service will respond to calls based on the following priorities: -

Priority 1 – e.g.; Breaches

Priority 2 – e.g.; Non authorised Information Sharing

Priority 3 – e.g.; Data protection advice and guidance

The Data Protection Officer Helpdesk can be contacted as follows: -

Email	schoolsdpo@wandsworth.gov.uk	Telephone	0208 871 8373

Data protection impact assessment (DPIA) enquiry form

Your name ....

Date form completed ....

Date form sent to data protection officer (DPO) ....

	DPOs: make any comments here
Please give a brief description of the project you are considering *(For example, purchase of online apps, or provision of IT services from an external provider)*	
Will this project involve the processing or sharing of personal data? *(Personal data is defined as any information that could identify individuals, such as names, contact details, user names or ID numbers)* YES / NO	
If 'YES', please give a description of what personal data you will be processing or sharing, and the scale of this processing	
Will this project involve the processing or sharing of sensitive personal data? *(Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometrics, physical or mental health, sexual orientation, or photographs)* YES / NO	
If 'YES', please give a description of what sensitive data you will be processing or sharing, and the scale of this processing	

Please return this form to your DPO.

DPO enquiry findings

For the DPO: complete this form outlining your recommendations and return to the appropriate person(s). Keep a copy for your records. Once the DPIA has been completed and sent to you, update this form and your records. In the event that a DPIA has not been undertaken, record the reasons in your records file.

Having reviewed the information submitted above, I recommend that a DPIA:	
IS required	
IS NOT required	
The reason for this decision is:	
I recommend that the DPIA is carried out by:	

Date findings concluded by DPO: ....

Signed by DPO:..

How to decide whether a DPIA is needed

A data protection impact assessment (DPIA) is required where a proposed data processing activity is likely to result in a high risk to people's rights and freedoms.

This checklist summarises the types of data processing activities to watch out for, based on DPIA guidance from the Information Commissioner's Office (ICO).

Types of processing that schools are more likely to carry out are highlighted in yellow. However, the other types listed here may still apply, depending on the scope of your activities.

Types of processing that ALWAYS require a DPIA under the GDPR

Type of processing	Example
Systemic and extensive profiling which result in a significant effect on the individual	• Credit checks • Mortgage and loan applications • Fraud prevention • Insurance underwriting • Application of artificial intelligence
Large-scale use of sensitive 'special category' data, or data on criminal convictions	• Trade union membership data • Health records • Social care records • Research projects • Political parties membership data • Fraud prevention • Application of artificial intelligence • Dating websites and applications
Monitoring of a publicly accessible area	• Audio/video surveillance of public areas e.g. CCTV • Automatic number plate recognition • Intelligent transport systems • Traffic management systems involving monitoring of vehicle and driver behaviour • Wi-Fi or Bluetooth tracking • Application of artificial intelligence to existing processes

Use of ‘new technologies’, or new uses of existing technologies	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearable devices) • Market research involving neuro-measurement (i.e. emotional response analysis)
Processing that could result in someone being denied a service, where it is based on automatic decision-making or involves the processing of special category data	• Pre-check processes related to contracts • Credit checks • Mortgage or insurance applications
Large-scale profiling of individuals	• Data processed by ‘Smart’ meters or ‘Internet of Things’ applications • Hardware and software offering fitness and lifestyle monitoring • Social media networks • Application of artificial intelligence to existing processes
Processing of biometric data	• Facial or thumbprint recognition systems • Building access systems • Identity verification • Access control and identity verification for hardware and applications (e.g. voice recognition, fingerprint and facial recognition)
Processing of genetic data (other than by a health professional to provide someone with medical care)	• Medical diagnosis • DNA testing • Medical research
Matching, combining or comparing personal data obtained from multiple sources	• Direct marketing • Monitoring use or uptake of statutory services or benefits • Fraud prevention

	• Federated identity assurance services
Invisible processing, where the data about a person has not been obtained from the person themselves	• Selling or purchasing lists of people and their data • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation and data aggregation platforms • Re-use of publicly available data
Tracking an individual's location or behaviour	• Data processing at the workplace • Data processing in the context of home and remote working • Social networks, software applications • Hardware and software offering fitness/lifestyle and health monitoring • 'Internet of Things' devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation and data aggregation platforms • Eye tracking • Processing location data of employees • Loyalty schemes • Tracing services • Wealth profiling – identification of high net-worth individuals for direct marketing
Targeting of children or other vulnerable individuals, particularly for marketing purposes, to create a profile of them, or if you intend to offer online services directly to them	• Social networks and applications • Connected toys

Processing that puts people at risk of physical harm if there was a data breach	• Whistleblowing/complaint procedures • Social care records

Types of processing that may not be high risk, but where a DPIA should still be conducted

Some processing activities may not fit the criteria for 'high risk' processing and therefore do not legally require a DPIA. However, it's good practice to conduct one whenever the way data is processed changes.

Data protection should be treated like any other risk, so DPIAs should be carried out in the same spirit as risk assessments or equality impact assessments.

If you're unsure whether to do a DPIA, err on the side of caution and conduct one.

Changes in school processes	• School mergers or closures • Introduction of remote working • New visitor sign-in systems
New technology purchased or implemented	• ICT hardware or software e.g. your management information system (MIS) • Changes to the ICT infrastructure e.g. moving to the cloud • New devices purchased e.g. tablets for lessons, laptops for staff
Changes to suppliers or service providers	• Switching catering or payroll providers

Data Protection Impact Assessment

Data Protection Impact Assessment for ____

Data set/system	Current practice	Impact of threat if occurs: 1=low 5=high	Likelihood: Low, medium, high	Response to risk	Action plan	Review date
Name the data set and/or system with personal level data	What current practices exist (or not) that could either lead to the threat materialising or prevent the threat from materialising? For example, data entry, data management, transfer of data, collection of data, printing and storing information, handling data	Identify what potential threat could be realised. Is threat related to: • Privacy breach (data shared w/o consent or disclosed) • Individual – in danger of harm/potential embarrassment /loss of confidentiality/ discrimination • System failure or technical issues • Non-compliance with GDPR through inadequate procedures/ non- consent/ negligence/ disregard/ ignorance/data shared without consent/data loss	As a result of practice, how likely is the identified threat a reality? Select from: Low Medium High	Transfer risk to third party/insurance Treat/mitigate Risk - reduce risk Tolerate/accept level of risk Terminate/remove risk	Where the likelihood of a threat is high or medium, identify the actions to address the threat and mitigate or minimise the risk if not eliminated What actions can be taken to minimise the risk or eliminate the risk altogether? In some cases, threats cannot be removed entirely in which case, can agree action to 'Accept risk – no further action necessary' Ensure actions have lead person identified, timelines and linked actions that impact upon the overall action to mitigate or eliminate the risk.	Depending on Action taken plan for a review

DPIA undertaken by ____ Date: ____________