LIGHTHOUSE SCHOOLS PARTNERSHIP

DATA PROTECTION POLICY

Statutory

Policy Approved by the Board of Trustees

Signed : A Hayson

Date: 11th December 2018

Name : Adele Hayson

Chair of Board of Trustees

Authorised for Issue

Signed :

Date: 11th December 2018

Name :

Chief Executive

Document History

Version	Author/Owner	Drafted	Comments
1.0	Clare Sanders/TJM	June 2016 Published 3-August 2016	Based on Gordano School model – original source not recorded
2.0	Louise Malik/Tim Monelle	August 2018	Updated to reflect GDPR and latest requirements

Date Policy Adopted	3rd December 2018
Review cycle	Biennial
Review date	Autumn Term 2020

This Policy applies to all schools and employees within the Lighthouse Schools Partnership.

DATA PROTECTION POLICY
Statutory

1. Aim

This policy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.
All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.

	Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all staff employed by the Trust, and to external organisations or individuals working on behalf of the Trust. Staff who do not comply with this policy may face disciplinary action.

5.1 Trustees/Local Governing Bodies

The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations. LGBs have responsibility for ensuring that their school(s) complies with the policies and procedures established by the Trust.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the Trust's compliance with data protection law, and developing related policies and guidelines where applicable. The Trust has appointed i-west to act as the DPO for a 3 year period from 1st June 2018.

i-west is part of the One West group, One West is the a Local Authority trading service that acts as a 'one-stop' shop for the provision of all independent assurance and governance services to an organisation.

The DPO will provide information to the Board of Trustees on compliance with the regulation along with their advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's service are set out in the Service Level Agreement (SLA) with i-west, attached to this policy as Appendix A. Contact details for the DPO are provided in the attached SLA.

5.3 Head of Trust Services

The Head of Trust Services acts as the representative of the data controller on a day-to-day basis.

5.4 Headteachers

Headteachers are responsible for ensuring that the Trust's data protection policies and procedures are implemented and maintained in their school(s) and that staff and LGB members have sufficient knowledge and training to carry out their responsibilities.

5.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust/school of any changes to their personal data, such as a change of address
- Contacting the DPO (using the DPO@LSP.org.uk email address, copying in the Headteacher for school based staff) in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR are based on data protection principles that the Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Trust will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted, ~~or~~ anonymised or pseudonymised. This will be done in accordance with the Trust's Records Management Policy.

8. Sharing personal data

The Trust will adhere to the principles of data sharing which are:

- Relevant
- Adequate
- Accurate
- Timely
- Secure

- Recorded where appropriate

In dealing specifically with data pertaining to Safeguarding issues the Trust shall adhere to the DfE guidance contained in *'Information sharing. Advice for practitioners providing safeguarding services to children, young people, parents and carers'* July 2018

The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The Trust will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised/ pseudonymised or consent has been provided

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of the Trust's pupils or staff.

Where personal data is transferred to a country or territory outside the European Economic Area, the Trust will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO using the DPO@LSP.org.uk email address, copying in the Headteacher for school based staff.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at a Trust Primary school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils above this age in a Trust Secondary school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

Requests for information must be made in writing; which includes email, and be addressed to the Data Protection Officer, Lighthouse Schools Partnership, c/o St Mary's Road, Portishead, Bristol, BS20 7QR, (DPO@lsp.org.uk). If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

When responding to requests, the Trust:

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one calendar month of receipt of the request

- Will provide the information free of charge. If the request is manifestly unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs. A reasonable fee may be charged if an individual requests further copies of their data following a request based on the administrative costs of providing further copies.
- May tell the individual that the Trust will comply within three calendar months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within one calendar month, and explain why the extension is necessary

The Trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information.

If the Trust refuses a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO (using the DPO@LSP.org.uk email address). If staff receive such a request, they must immediately forward it to the DPO email address.

10. Parental requests to see the educational record

There is no automatic parental right of access to the educational record of children and young people attending academies. However, the Trust's policy is that Parents, or those with parental

responsibility, may have reasonable access, free of charge, to their child's educational record within one calendar month of receipt of a written request to the DPO email address (DPO@LSP.org.uk).

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school lunch instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

Please note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Parents/carers will be notified before any biometric recognition system is put in place or before their child/young person first takes part in it. The Trust/school will obtain written consent from at least one parent or carer before any biometric data is taken from their child/young person.

Parents/carers and pupils have the right to choose not to use the Trust's/school's biometric system(s). The Trust will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school lunch using a cash top up card if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the Trust/school will delete any relevant data already captured.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the Trust will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the Trust/school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust/school will delete any relevant data already captured.

12. CCTV

The Trust may use CCTV in various locations across the Trust to ensure the safety and security of the sites and of all users of the sites. We will adhere to the ICO's code of practice for the use of CCTV.

The Trust does not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras, where in use, will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO using the DPO email address (DPO@LSP.org.uk).

13. Photographs and videos

As part of our Trust/school activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent (for pupils aged under 18), we will clearly explain how the photograph and/or video

will be used to both the parent/carer and pupil. Where we do not need parental consent (for pupils aged 18 or over), we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within Trust/school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of the Trust/school by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust or school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way the Trust/school will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14. Data protection by design and default

The Trust will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Trust/school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the Trust/school office
- Passwords that are at least eight characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Users are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, Trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment. This is detailed in the Acceptable Use Agreement that all Trust staff are required to sign. This is provided in the Code of Conduct Policy.
- Where we need to share personal data with a third party, we carry out a risk based assessment for each type of recipient, follow due process and take reasonable steps to ensure it is stored securely and adequately protected.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

A 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix C.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an education context may include, but are not limited to:

- A non-anonymised dataset being published on the Trust/school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop containing non-encrypted personal data about pupils

18. Training

All staff, Trustees and governors are provided with computer based data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The Head of Trust Services is responsible for monitoring and reviewing this policy, in conjunction with the DPO.

This policy will be reviewed every two years by the Board of Trustees.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable Use Agreement
- Records management policy and guidelines.

Appendix A

Data Protection Officer Service Level Agreement

Objective of the Agreement

The purpose of this Service Level Agreement is to describe the key services we provide and the quality standards we have agreed with our service users in terms of service delivery.

This Agreement sets out

- the services we provide to our partner organisations
- the overall standard which we aim to achieve in the provision of our services
- a mechanism for resolving any problems relating to the delivery of the service

Future reviews and amendments to this Service Level Agreement

This agreement will be reviewed annually as part of the annual planning process and any changes will be agreed with service users. Changes made to this agreement will be signed off by all parties where changes occur.

Objectives of the Service

To provide an effective Data Protection Officer support service role including additional assistance through training and advice for GDPR compliance

Service Users

Insert name of the other parties to this agreement i.e. school

Responsibilities - who we are, what we do

i-west will act as your Data Protection Officer, reacting to incidents and providing assistance through specific training and direct contact through our email i-west@bathnes.gov.uk

Service Availability

In order to effectively manage your requests for assistance please contact i-west@bathnes.gov.uk for assistance. This email account is managed effectively and matters will be dealt with urgently where appropriate. If the matter is of an urgent matter such as a potential breach please call

01225 395959

Description of key services

i-west as part of the agreement will

- Conduct 4 compliance visits (1 at the Trust , the rest at your choosing) Remaining academies will be asked to submit self-assessment documents
- Respond to general queries
- Advise on dealing with subject access request
- Assist on Data Protection Impact Assessments
- Advise on Information Sharing Agreements
- Review Policies and Procedures of requested
- Manage incidents
- Act on your behalf as a your point of contact with any communication with the regulator (Information Commissioners Office);
- Provide access to training events throughout the year;
- Provide you with use of our high quality e-learning modules on Data Protection through our website;
- Provide you with our Information Governance newsletters throughout the year;
- Attend at Board Level or Senior Management meetings to present findings of our Data Protection review where required;

Monitoring success

Our team of professionals throughout the year will ensure that you get the highest quality support and through management we will ensure that this is maintained. All of our staff are highly trained and reviews of the output of work will be conducted to ensure continued effectiveness.

Data processing agreement

- We will process personal data on your behalf for the purpose of providing you assurance on your Data Protection Compliance.
- The condition for processing such data is for the performance/delivery of this agreement.
- We keep your data for **3** years or for the duration of the agreement (whichever is less).
- We maintain appropriate technical and organisational measures to ensure your data remains secure.
- We do not share your data with any other organisation unless required to by law.

Complaints

Any complaints to the service will need to be reported directly to 01225 395959. We will investigate any complaints in detail and ensure a satisfactory conclusion.

Date of Agreement (insert date)

1st June 2018

Signatories to Agreement

- (Include details of all parties to the agreement - all parties should sign this agreement)

LIGHTHOUSE
SCHOOLS PARTNERSHIP

Appendix B

Personal data breach procedure

In the event of a suspected personal data breach, the following procedure should be followed:

1. Report the potential breach, as soon as possible, to the Data Protection Lead and/or Headteacher of the school in which the potential breach has occurred.
2. The Data Protection Lead and/or Headteacher of the school will then report to the potential breach to the Trust using the email address DPO@lsp.org.uk. This will also be shared with the Trust's Data Protection Officer (DPO), provided by i-west.
3. The Headteacher of the school in which the potential breach has occurred will complete an incident report. The incident report will document the facts relating to the potential breach, its effects and any initial remedial action to be taken. The completed incident report should be shared with the Trust via DPO@lsp.org.uk. A template incident report can be found in Appendix D.
4. With the information in the incident report, the DPO will ascertain if a breach of personal data has occurred. A personal data breach is one which, if not addressed in an appropriate and timely manner, may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.
5. The DPO will try to contain the breach and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.
6. If it is likely that there will be a risk to people's rights and freedoms as a result of the breach then the DPO will report the breach to the Information Commissioner (ICO) within 72 hours. In these cases, the DPO will also inform those concerned directly and without undue delay.
7. The Trust will investigate every breach of personal data to identify whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.
8. Any changes to procedures, advice or additional training requirements will be shared with leaders and staff in the Trust as appropriate.

Appendix C

[SCHOOL NAME]

Information Potential Data Breach Response – Record of work

This document provides the documented evidence and audit trail of a reported potential data breach. It is designed to operate alongside the LSP's Data Protection Policy, and Personal data breach reporting process.

This form is to be completed by the Incident Handler(s) in the school. The Incident Handler will usually be the school's data lead and/or the Headteacher

The incident may require additional input and support from other organisations such as ICT, the school's Data Protection Lead, The LSP's DPO and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Date incident occurred:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to incident handler:	
By whom:	
Date reported to the Trust:	
By whom:	
Date DPO informed:	
By whom:	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment	

Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	*If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay* **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned **Decision to report to ICO** - Yes / No Based on: Officer: Signed: Date: