Midsomer Norton Schools Partnership

Issued: September 2022
Review: Term 1 annually
LST: CHO

DATA PROTECTION and DATA BREACH POLICY

Contents

The Midsomer Norton Schools' Partnership (known from now on as the 'Trust') is committed to the protection of all personal data that it collects, stores and processes about pupils, parents, carers, school workforce (including governors and volunteers), visitors and other individuals. This policy applies to all personal data regardless of its format.

The Trust must process personal data according to the Data Protection Principles set out in the Data Protection Act 2018. This requires the Trust schools to collect and use data fairly, to store it safely and not to disclose it to any other person unlawfully. The requirement for the Trust to comply with this Act, in protecting the rights and privacy of individuals, imposes certain responsibilities on those who have access to the data, to understand their responsibilities and the implications of data misuse.

Please refer to the following appendices:

1 Purpose and Scope

Schools in the Trust need to collect and use certain types of information about people with whom they deal in order to perform their functions. This includes information on current, past and prospective pupils and employees, suppliers, clients, customers, service users and others with whom they communicate. The Trust is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. There are safeguards to ensure this in the EU General Data Protection Regulation.

The Trust regards the lawful and correct treatment of personal information as critical to successful operations, and to maintain confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly and is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 2018, (DPA).

This policy links with other Trust policies including; Freedom of Information and Information Access Policy, Records Management Policy, ICT Policies including Email and Internet Use Policies, Employee Code of Conduct, Human Resources Policies, Criminal Records Bureau Staff checks (Disclosure and Barring Service) Policy and Procedures.

2 Legislation and Guidance

This policy meets the requirements of the General Data Protection 2018 (hereafter referred to as GDPR), the Data Protection Act 2018 (hereafter referred to as DPA) and is based on guidance published by the Information Commissioner's Office (hereafter referred to as ICO) and the ICO's Code of Practice for Subject Access Requests and Reporting of Data Breaches.

The policy also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

The Trust has adopted the Information and Records Management Society's guidelines for Schools regarding the storage and destruction of personal information.

The Midsomer Norton Schools' Partnership Trust is the Data Controller for the purposes of GDPR and DPA and is registered with the ICO (Registration No.Z249097X).

3 The Role of the Trust

The CEO is the data controller under the DPA and is ultimately responsible for implementation of the DPA. This role may be delegated to another senior member of the MNSP Central Team. The Trust has appointed the COO as the Data Protection Officer, who provides the Trusts primary contact to the Information Commissioner, and is responsible for ensuring provision of suitable DPA advisory, training and awareness services, DPA request handling, ensuring compliance with Information Commissioner, and for keeping the Board of Trustees aware of relevant DPA issues.

4 Governance

This policy has been approved by the Board of Trustees and it will be reviewed annually with other policies and guidelines as set out by the Board of Trustees.

5 Rights of staff, students and third parties

The Trust will ensure that the rights of people about whom the information is held can be fully exercised under the Regulation.

Schools within the Trust will provide individuals with a copy of the information held about them within one month of receiving a request (subject access). This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. On receiving a subject access request the individual school will check and require evidence of the identity of the individual and any further information required to isolate the records of that individual. Where a subject access request has a broad scope, the individual school may ask for more details from the data subject in order to locate the information that is of particular interest.

Where a large volume of information is held, the individual school may seek to make the information available in ways other than providing a copy. This could include arranging an appointment for the data to be inspected within the school. In addition to the personal data itself, the individual will be provided with any supporting information that is needed to understand the data held, and the processing of it.

Where information located as part of a subject access request (section 15) contains personal data about a third party, information will not be released unless the requirements set out in section 9.1 are met. The introduction of the right of access to non-personal information held by the school under the Freedom of Information Act 2000 may also need to be considered. This is because some requests may be for a combination of personal and non-personal information.

The Trust will comply immediately with a request from an individual to cease sending them marketing or consultation information.

Requests from individuals to correct, rectify, block, or erase information that they regard as wrong information or to stop processing that is causing damage or distress will be considered by the individual school on a case by case basis. The individual concerned will be fully informed of the resulting decision and the reasons for it. Legal advice will be sought by The Trust should a request not be supported, or if considered sensitive/complex, before coming to a decision.

An individual wishing to exercise any of their rights under the GDPR should put their request in writing to the school.

6 Roles and Responsibilities

<u>Trust Board and Local Governing Body</u>
The Trustees have overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

<u>Data Protection Officer</u>
The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

<u>Headteacher(s)</u>
The academy headteacher(s) act as the representatives of the Data Controller on a day-to-day basis.

<u>School Workforce</u>
The school workforce, for the purpose of this document, is defined as school staff including governors and volunteers. The school workforce are all responsible for:

- collecting, storing and processing any personal data in accordance with this policy;
- informing the Trust of any changes to their personal data, such as a change of address;
- contacting the DPO 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, or they suspect, a data breach;
- whenever they are engaging in a new activity, including the procurement of new technologies or equipment, that may affect the privacy rights of individuals;
- if they need help with any contracts or sharing personal data with third parties.

7 Data Protection Principles

Personal data must be:

- used lawfully, fairly and transparently;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure.

8 Collecting personal data

The Trust collects and processes personal data where they have a lawful basis (legal reason) to do so under Article 6 of GDPR. The lawful bases are:

- Contract - the data needs to be processed to fulfil a contract between the Trust and an individual, or where the individual has asked the Trust to take specific steps before entering into a contract;
- Legal obligation - to comply with the law i.e. Education Act 1996;
- Public interest - to allow the Trust to perform a task in the public interest or official function when providing education;
- Vital interests - to prevent someone from being seriously harmed or killed;
- Legitimate interests - to collect and process information necessary (except when unfair to an individual). The Trust has a legitimate interest in:
  - providing an education;
  - safeguarding and promoting pupil welfare;
  - promoting the objects and interests of the Trust. This includes fundraising and marketing through school website, social media and school prospecti;
  - ensuring the efficient operation of the Trust and that all relevant legal obligations of the Trust are complied with;
- Consent - where the Data subject (or their parent/carer when appropriate e.g. where the pupil is under the age of 13) has freely given clear consent.

The Trust collects and processes special categories of personal data. Where this is necessary the Trust will also meet one of the special category conditions for processing which are set out in Article 9 of the GDPR.
Special category conditions are:

- Substantial public interest - where processing is necessary for reasons of substantial public interest;
- Vital interests - to protect a pupil where they are unable to give consent e.g. if they are seriously hurt or/and are unconscious;
- Legal claims - where processing is necessary for the establishment, exercise or defence of legal claims. This allows the Trust to share information with their legal advisors and insurers;
- Medical purposes - this includes medical treatment and the management of healthcare services e.g. immunisations, school nurse etc.;
- Explicit consent - The Data subject (or their parent/carer when appropriate e.g. where the pupil is under the age of 13) has freely given explicit consent;
- Archiving purposes in the public interest.

The Trust will only collect personal data for specified, explicit and legitimate reasons. The reasons for collecting data is explained to Data Subjects and/or their parent/carer when we first collect their data (usually on employment, admission or if

associated with governance for example). A copy of the Trust Privacy Notices are published on the Midsomer Norton Schools' Partnership website under Partnership Policies.

If the Trust wants to use personal data for any other reasons other than those given when we first obtained it, or in subsequent privacy notices, it will inform the individuals concerned, and seek consent where necessary, prior to processing.

Staff must only process personal data where it is necessary in order to do their jobs. Personal data that has been processed must be either archived, anonymised or destroyed as soon as possible.

9 Disclosure and Sharing Personal Data

9.1 Third party access to information

Where a request for personal data is made by a third party on behalf of the data subject it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

Occasionally, third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the school will consider the following:

- any duty of confidentiality owed to the third party;
- attempts to get consent from the third party;
- any express refusal of consent from the third party;
- the third party's expectations with respect to that data.

When a request for personal data is made by a third party and not on behalf of the data subject, the individual school shall consider the request under Freedom of Information as well as GDPR. It shall consider whether releasing the personal data would breach any of the Data Protection principles and in particular whether any exemptions under GDPR apply. Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation.

The Freedom of Information policy deals with requests for information about third parties, and information will be withheld where disclosing it would breach any of the Data Protection principles. Where a requester does not state a specific reason for requesting the information then the FOI policy should be followed. When there is a specific reason for requesting the information, an exemption under GDPR may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax. If an appropriate exemption under GDPR does apply so that the Data Protection principles will not be breached, the school will usually comply with the request. However, without a Court Order there is no obligation on the school to disclose the information.

Where the individual school is not convinced that the third party has entitlement to the personal data, or that any exemptions under GDPR apply, and that releasing information would breach the Data Protection principles, the personal data will be withheld and only released on presentation of a Court Order.

9.2 Information sharing

The Trust promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (GDPR exemption exists) to allow the sharing of such information.

The Trust will ensure that supporting processes and documentation are made available to professionals so that they understand how to share information safely and lawfully. Where an employee acting in good faith, has shared information in accordance with these supporting processes and guidance, they shall not normally be subject to disciplinary action.

Sharing large sets of information, or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the GDPR and that additional safeguards can be considered and put in place.

9.3 Contractual and partnership arrangements

When a school within the Trust enters contractual or partnership arrangements which involve the processing of personal data, a written agreement will specify which party is data controller or whether there are joint data controller arrangements. Where a third party is processing personal data and information on behalf of the school, a written contract will be put in place. Specific care will be taken in respect of services provided online and via 'the cloud'.

Where the school remains as data controller, it will take steps to ensure that the processing by its contractors and sub-contractors will comply with GDPR. Contractors will not be able to sub-contract Data Processing without the explicit written permission of the school. Staff will take reasonable steps to ensure that data processing by third parties is regularly monitored to ensure GDPR requirements are being met.

Where the parties are data controllers jointly or in common, the school will liaise with the other party to ensure that all processing complies with GDPR. The responsibilities of each data controller should be expressly and clearly laid out.

All contractors who are users of personal information supplied by the school will be required to confirm that they will abide by the requirements of the Regulation to the same standard as the school with regard to information supplied by the school. Staff should obtain advice from Legal Services as necessary. All contractors, consultants, partners or agents of the school must ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the school, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of the contract between the school and that individual, company, partner or firm. The school shall take reasonable steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf.

Any observed or suspected security incidents or security concerns should be reported to the school. All contractors, consultants, partners or agents of the individual schools must allow data protection audits by the school of data held on its behalf if requested in line with these contractual arrangements.

NB: It is expected that all contractors, consultants, partners or agents of the individual schools must indemnify the school against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

10 Subject Access Request

Please refer to the MNSP **Subject Access Request Policy**

All Subject Access Requests (SAR) or enquiries about accessing personal data should be referred to the DPO in the first instance.

A SAR, is a written request for personal data held by the Trust about an individual, or Data subject. Generally, individuals have the right to see what personal data the Trust holds about them and are entitled to be given a description of the information, what it is used for, who it is shared with and how the Trust protects, stores and destroys the individual's personal data.

A SAR does not have to be submitted on an official form but as personal data can be complex, and include information held both electronically and manually, it is advisable to complete the Trust's Subject Access Request form. Completing the form should ensure that the Data Protection Officer has sufficient information to process the request within the official timescales.

Checking of Identity

On receipt of a SAR the DPO will need to establish the requestor's identity to ensure that information is not accidentally sharing another person. It may be necessary therefore, to ask the requestor to provide documents to evidence their identity. Details of acceptable identification documents are included on the form.

10.1 Children and subject access requests

Children under the age of 13 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/carers of pupils under the age of 13 may be granted without the express permission of the pupil.

If a Subject Access Request is received from a parent/carer of a child aged between 13 and 16, the DPO will need to consider whether the child can provide their consent to the parent/carer acting on their behalf. The DPO will also consider whether the child understands why the Subject Access Request is being made and whether they are able to understand the information that they will receive. If a Subject Access Request is made for a child over the age of 16, the child will be

required to give consent. The Trust will automatically supply any report of student progress without reference to the child whilst on role at any school.

If the person requesting the information is a representative of the Data Subject then the representative must supply proof of the Data Subject's consent for the release of their personal data, or an explanation of why they are entitled to make the request. An individual appointed to act for someone under the Mental Capacity Act 2005 must confirm their capacity to act on the Data Subject's behalf and explain how they are entitled to access the information.

10.2 Rights of data subjects to access personal data

GDPR states an individual, or Data Subject, has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her is being processed. Where that is the case, the Data Subject is entitled to make a written request to access their personal data and ascertain the following:

- categories of their personal data processed;
- purposes of the processing of their personal data;
- recipients, or categories of recipients, to whom their personal data has or will be disclosed;
- period for which their personal data may be stored;
- where their personal data has not been collected directly from the Data subject, any available information as to the source of that data;
- the existence of any automated decision making and information about that decision making;
- If personal data is transferred to a third country or to an international organisation the Data subject is entitled to be informed about the appropriate safeguards which have been made relating to the transfer.

The Data Subject also has the right to request a Data Controller to rectify incorrect personal data, and in some circumstances the Data Subject may be able to object to and restrict processing of personal data or ask for its erasure. Data Subjects have the right to lodge a complaint with the ICO.

Data Subjects include all staff and students of the Trust and any other person about whom the Trust holds and processes personal data (third parties).

10.3 Opt out rights

The Trust may not always seek the consent of data subjects when processing personal data, for example, when processing for normal business purposes or when the information is already in the public domain.

If any person has good reason for wishing their details to remain confidential in any such instance, they should contact the Data Protection Officer for the Trust.

11 Validation and collation of information

An individual is only entitled to personal data about themself. Therefore, if the personal data includes information about someone else, the Trust will need to redact the information about a third party before supplying the personal data to the individual making the subject access request; in some cases it may not be possible to supply such data and the Trust may be able to decline to providing the data.

If responding to a Subject Access Request may involve providing information which relates to the individual and in doing so include a third party, then the Trust does not have to comply with the request if it would mean disclosing material about the other individual. Material qualifies as third party information either if the other person can be identified as the source of the information, or if they are just included in it e.g. as a witness. However, third party material is not automatically excluded and the Trust would be able to provide the information about another other person if:

- that person has given their consent; or
- it is reasonable to go ahead without their consent.

In deciding whether it is reasonable to go ahead without consent, the DPO would take account of:

- any duty of confidentiality the Trust owes to the other person;
- anything that the Trust has done to try and get their consent;
- whether they are able to give consent;
- whether they have refused consent.

Before sharing any information that relates to third parties, the Trust will where possible, anonymise information that identifies third parties not already known to the individual (e.g. Trust employees), and redact information that might affect the third parties privacy. The Trust may also summarise information rather than provide a copy of the whole document. GDPR requires the Data Controller to provide personal information not documents.

Information that is subject to legal professional privilege may be held back – this protects communications between lawyers and their clients for the purposes of giving or obtaining legal advice and communications between lawyers, clients and third parties made for the purposes of litigation, either actual or contemplated.

12 Responsibilities and Penalties

12.1 Persons who process personal data on behalf of the Trust

Anyone who processes (stores or uses) personal data on behalf of the Trust has a responsibility to ensure that the Data Protection Principles are observed. Detailed advice on how to achieve this is given in the Data Protection Policy Guidelines, which summarise detailed guidance from the Office of the Information Commissioner or the JISC Code of Practice.

12.1.1 Staff

Staff who, as part of their responsibilities, process personal information about other people (for example, about students' course work, personal circumstances of other members of staff or research data from human subjects), must comply with this Data Protection Policy.

12.1.2 Students

Students who are considering processing personal data as part of their studies, must notify and seek approval from their teacher before any processing takes place.

12.1.3 Others working for and on behalf of the Trust

Others working for and on behalf of the schools within the Trust (usually called third parties), who handle personal data in connection with the Trust should operate in accordance with the DPA and details of any such processing should be subject to written agreements between the Trust and the third party. Such third parties include external supervisors, external examiners, suppliers or customers.

12.2 Persons who provide personal data to the Trust

Everyone who provides personal data to the Trust is responsible for ensuring adherence to the Data Protection Principles, especially with regard to accuracy and, in the case of third parties providing the personal data of others, the right to disclose this personal data.

12.3 Penalties

It is a criminal offence to access personal data held by the Trust for anything other than school business, or to procure the disclosure of personal data to a third party. It is a further offence to sell such data.

Employees who access or use personal data held by the school for their own purposes will be in breach of relevant policies of the Trust, including but not limited to, the Employee Code of Conduct, Social Media Policy, ICT Policies and subject to disciplinary action, which could include dismissal.

13 Data Quality, Integrity and Retention

- Personal data held will be relevant to the stated purpose and adequate but not excessive.
- The Trust will ensure, as far as is practicable, that the information held is accurate and up-to-date.
- If personal data is found to be inaccurate, this will be remedied as soon as possible.
- Personal information, such as contact details, may be shared within the school/Trust where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.
- Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.
- The use of personal data by the schools within the Trust will comply with the Trust Records Management Policy and Retention Schedules covering every type of school record.
- Information will only be held for as long as is necessary after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.
- Redundant personal data will be destroyed using the Trust's procedure for disposal of confidential waste and in accordance with retention schedules.

14 Security

Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with ICT security arrangements and policies may result in disciplinary action, including dismissal.

The Trust will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information. An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

The Trust has a range of ICT Policies covering the use and access to data which apply to electronic systems containing personal data. All staff within the Trust will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

All data breaches (however minor) should be reported to the headteacher of the relevant school in the first instance. Details of the breach must be logged on the appropriate reporting form and shared with the Data Protection Officer and the Trust PA.

Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices. Where staff have access to laptops, the user accounts will not allow the installation of additional software or change security settings. This will prevent the inadvertent installation of malicious or dangerous scripts, viruses or ransom ware. Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

Employees who process personal data out of the school (e.g. on another site, at home) can only do this with the express consent of their headteacher. Access to personal data outside of the school should not be attempted using unsecured access systems (this includes via mobile networks outside of UK unless the network has been checked in advance to be compliant under data protection law).

System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data. Personal data will not be transferred outside the

European Economic Area without the approval of the data controller, this includes any school trip to a country outside of the EEA. If in doubt, contact the DPO before any data is transferred.

14.1 Paper-based records that contain personal data must:

- be kept in a secure locked cupboard/office when not in use;
- not be left unattended on office and/or classroom desks;
- not be pinned to notice/display boards in areas;
- not be stored, or left, in any areas where anywhere pupils, parents/carers or visitors will be left unattended.

Where documents containing personal information need to be taken off site, staff must ensure that documents are not left unattended at any time and are returned to secure storage at the trust premises at the earliest possible opportunity.

14.2 Electronic records that contain personal data must:

- only be viewed on devices that are protected by strong passwords, automatic screen locking and up to date security software;
- not be downloaded onto portable storage devices and/or personal devices. The use of removable media such as USB is not allowed.

Trust devices are subject to regular enforced password changes which meet the Trust's criteria for strong passwords which are based on current industry best practice guidance.

Portable devices issued by the Trust should be encrypted and it is the responsibility of the user to ensure that devices are returned to IT Support for any security updates when requested to do so.

Documents and folders that contain personal data should only be sent or shared:

- as a link to a Google document which has appropriate sharing and security rights;
- as an encrypted, or password protected, attachment if sent externally; If an external agency requests that data is sent in an unencrypted manner (eg the Passport Office), this MUST be discussed with the DPO before data is sent.
- through a secure data sharing portal such as Globalscape;
- or via the school's electronic communication system (PARS or Insight).

Staff and governors who access personal information on their personal devices are expected to follow the same security procedures as for trust-owned equipment (see suite of related ICT policies for further information). Documents should be only viewed and not downloaded to personal devices. Security settings on Google documents can be set to restrict downloading and printing of documents as required.

15. Subject Access Requests and Data Protection Complaints

Subject access requests and data protection complaints should be addressed to:
Mr Alun Williams, CEO, Midsomer Norton Schools Partnership, c/o Norton Hill Primary School, Silver Street, Midsomer Norton, BA3 2UD. The request will be passed to the DPO who will acknowledge the application in writing. Once any queries around the information requested and identification have been resolved the Trust will normally have 30 days to respond to the request.
Where the Subject Access Request was made by electronic means, and unless the Data subject requests otherwise, the information will be provided in a commonly used electronic form. Where this it is impossible, or where it would involve undue effort, to complete a data request, an alternative would be to allow the requestor to view the information on screen at the Trust's premises. Information will not be disclosed by fax or telephone. Disclosure by post is usually made by first class post to the address provided or, if appropriate, to a named representative.

Complaints about schools in the Trust processing of personal data and rights under the General Data Protection Regulation will be dealt with in accordance with this policy and Trust complaints policy.

Individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the General Data Protection Regulation. If individuals are not happy about how the Trust have handled their information they can contact the ICO via the following means:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Alternatively visit their website - www.ico.gov.uk or contact them by phone on 03031231113. The Trust will respond promptly and fully, to any request for information about data protection compliance made by the Information Commissioner.

The Trust will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the school by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to Parliament.

18. Other data protection rights of the individual

In addition to the right to make a subject access request individuals also have the right to:

- withdraw their consent to processing at any time (in certain circumstances);
- 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. If staff receive such a request, they must immediately forward it to the DPO.

19. Parental requests to see the educational record

Parents/carers, or those with parental responsibility, have a legal right under the Education (Pupil Information) (England) Regulations 2005, to access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

20. Photographic Images and Video Footage

Photographic images and video footage of individuals may be processed by the Trust. This includes CCTV footage for the purpose of ensuring the safety and security of pupils, school workforce and visitors (see the Trusts' CCTV policy for further information). It also includes the use of photographs taken by the school photographer to be used in the Schools MIS system and for internal school promotion.

The Trust assumes that by accepting the home school contract and sending their child to the school, they are accepting that photographic images can be used within the school (e.g. on school notice boards). This is the contract that you agree to and is not consent.

If photographic material is to be used in any form of external communication then written consent will be obtained from all relevant parents/carers for the photographs and videos that are to be used for communication, marketing and promotional materials. When obtaining consent it is explained how the image or footage photograph will be used by the Trust.
Consent can be granted or withdrawn at any time. If consent is withdrawn, the Trust school will delete the photograph or video and not distribute it further.

Where consent has been given to use images or footage, the Trust will only provide minimal information on pupil i.e. first name only, unless the Data subject, or their parent/carer, has agreed otherwise.

21. Disposal of records

Personal data that is no longer needed must be disposed of securely. Personal data that has become inaccurate, or out of date, will also be disposed of securely where it cannot or does not need to be rectified or updated.

Staff who are responsible for archiving pupil and staff files (electronic and paper) must familiarise themselves with the Trust's Data Retention Guidelines before disposing of any personal data.

In exceptional circumstances it may be necessary to retain data beyond the retention period. This may be in response to the Trust receiving notification of legal proceedings or legal action (or potential legal action), government or regulatory investigation or complaints or claim against or involving the Trust. In the event of such an occurrence the data should be flagged with the DPO and all relevant date retained and flagged with "DO NOT DESTROY THIS DATA". If there is any doubt over whether data should be retained or destroyed then the DPO should be consulted.

Where it is then agreed that personal data has reached the end of the retention period (see Records Retention Policy), and does not need to be kept for any of the exceptional circumstances detailed as above, it should be destroyed by the following method:

- Electronic files and emails containing personal data must be reviewed regularly. If the personal information is no longer required, and does not need to be retained, it should be deleted. If the information needs to be retained it should be attached electronically to the Trust's Management Information System (SIMS) or archived according to the retention guidelines;

- Paper based records containing personal data must be disposed of in the confidential shredding bins provided by the Trust;

- Printer films and tapes containing personal data will be placed in a sealed envelope and stored in a secure locked cupboard/safe for disposal with the contractor responsible for confidential shredding bins. A separate certificate will be issued for their disposal.

- Defunct IT hardware containing personal data will be disposed of by a specialist IT disposal contractor, a certificate will be required to prove correct disposal.

- Hard drives, which have been removed and stored for reuse, will have any data erased be before being moved to secure locked storage.

- Backup tapes, if used, containing personal data will be deleted, or overwritten, when the stored data has reached the end of its retention period.

The Trust contracts third party disposal companies to securely dispose of paper documents, IT consumables and equipment that contain personal data. Companies who provide confidential waste services must provide evidence of their GDPR compliance and provide certification of disposal.

22. Data Breach

22.1 Definitions / Types of breach

Data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Trust's information assets and / or reputation.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

22.2 Reporting an incident

Any individual who accesses, uses or manages the information systems run by the Trust is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer or to the Headteacher. This report should be both verbally and in writing. There is a process chart in Appendix 1 to assist with the reporting process.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 2).

All staff should be aware that any breach of Data Protection legislation may result in the Trust's Disciplinary Procedures being instigated

22.3 Containment and recovery

The Data Protection Officer (DPO) or Headteacher will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO or Headteacher in liaison with other relevant staff to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO). The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate. Advice from experts may be sought in resolving the incident promptly. The LIO, in liaison with the relevant staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

22.4 Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved;
- its sensitivity;
- the protections are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen;
- whether the data could be put to any illegal or inappropriate use;
- Data Subject(s) affected by the breach, number of individuals involved and the potential effects on those Data Subject(s);
- whether there are wider consequences to the breach.

22.5 Notification

The LIO and / or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation[1];
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the University for further information or to ask questions on what has occurred.

The LIO and / or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. 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.

The LIO and or the DPO in conjunction with the CEO will consider whether there should be a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

22.6 Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.
- If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by Trust Board.

22.7 Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

[1] [1] Individual Rights: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individualrights/

23. Implementation

The responsibility for implementation of this policy rests with the individual schools within the Trust.

Each school will ensure that:

- Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and/or handling personal information is appropriately trained to do so.
- Everyone managing and/or handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is given advice as necessary.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Employees are aware of the action required in the event of a Data Breach.

On joining the Trust, employees are required to undertake training on Data Protection and ICT Security as part of their induction. They will not be allowed to use the school's network until successfully completing the training.

The Data Protection Officer works with schools within the Trust to maintain the on-going programme of annual training and awareness to maintain a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

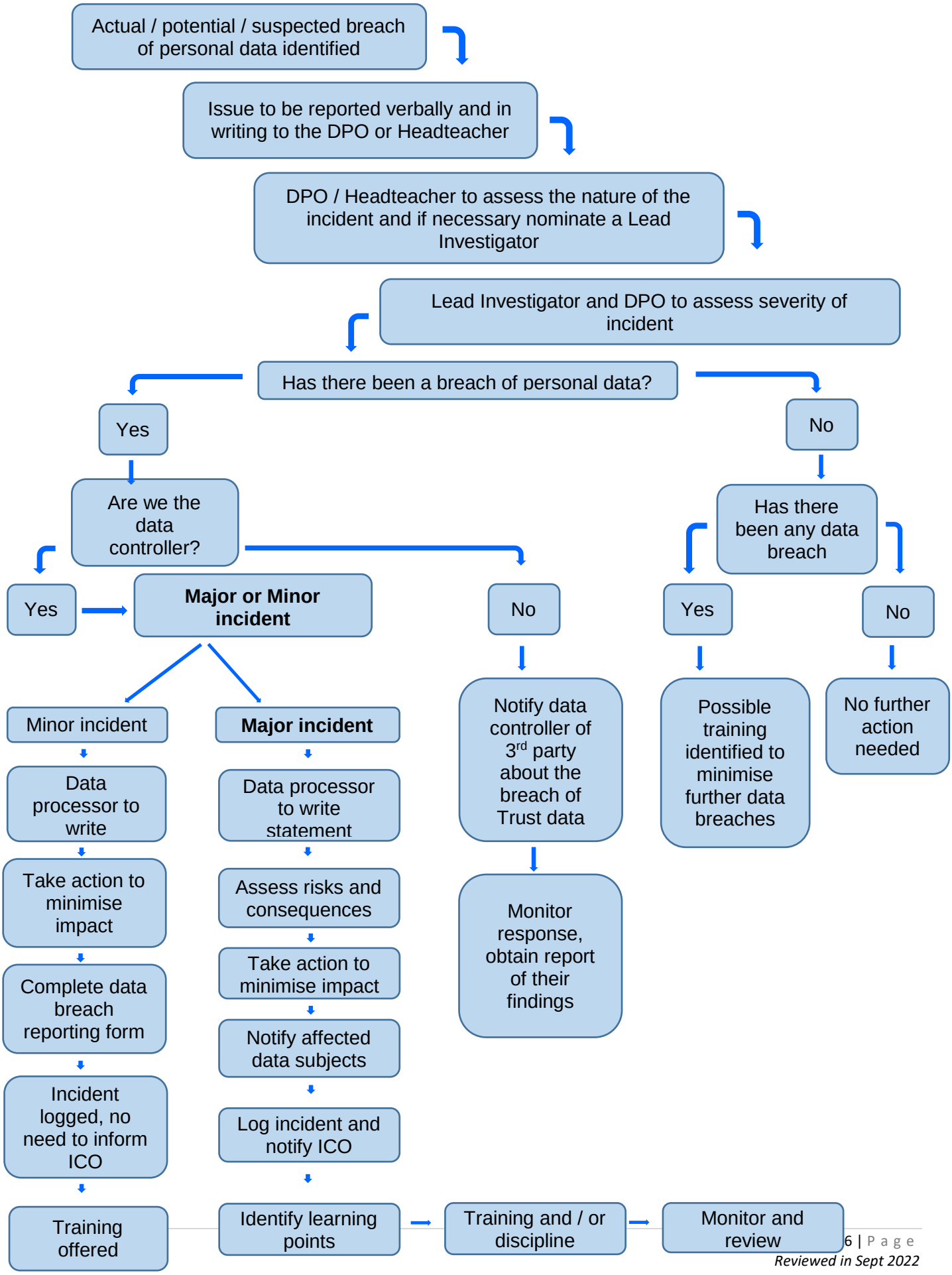
Supporting procedures for this policy have been created and are maintained within the Policy and Guidance pages that are available on the Trust website. Appropriate levels of consultation takes place at review time before the Trust Trustees approve the changes for implementation.

Data Protection audits regularly carried out by internal audit (external audits may be commissioned if required) in order to monitor compliance with the GDPR and this policy.

The Board of Trustees receive a report on data breaches at their termly meetings.

Data Breach Policy

Data Breach Process



GLOSSARY OF TERMS

Many of the definitions in this glossary are based on the key definitions from the Office of the Information Commissioner. The full definitions together with further information and useful examples can be found on the Key Definitions webpage of the Office of the Information Commissioner's website.

DPO – Data Protection Officer
DPA – Data Protection Act
GDPR – General Data Protection Act
ICO – Information Commissioner's Office

Personal data

Personal data means data which relate to a living individual who can be identified -

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Within the Trust, personal data, sometimes also called personal information, is any information about a living individual that can be used, either on its own or in conjunction with other information held by the Trust or other information likely to come into the possession of the Trust, to identify that person. It includes any expression of opinion about an individual and any indication of the intentions of the Trust in respect of the individual. It includes information stored in any medium: paper and electronic, text, image, audio and visual.

Data controller

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

In the case of the Trust, the Executive Headteacher is the data controller. He has delegated this role to the Data Protection Officer who determines the purposes for which, and the manner in which, any personal data are processed or are going to be processed. This includes being responsible for destroying the data when no longer relevant. Individual members of staff or students, who process data on behalf of the Trust, are data users. Personal data should always be processed according to the Data Protection Principles

Data processor

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

In the case of the Trust, a data processor is any person within the schools within the Trust that processes data or disposes of confidential waste on behalf of the Trust.

Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -

a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data.

Processing of personal information includes collecting, using, storing, destroying and disclosing information.

The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing

Data Protection (DP) Principles

The Data Protection Act (1998) sets out eight Data Protection Principles. In summary these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for those purposes;
- be accurate and kept up to date;
- not be kept for longer than is necessary for that purpose;
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised access, accidental loss or destruction;
- not be transferred to a country outside the European Economic Area, unless that country has adequate levels of protection for personal data.

Also, further details are given by the Office of the Information Commissioner and the Ministry of Justice.

Data subject

Data subject means an individual who is the subject of personal data.

In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Sensitive Personal Data

Sensitive personal data means personal data consisting of information as to -

a) the racial or ethnic origin of the data subject,
b) his political opinions,
c) religious beliefs or other beliefs of a similar nature,
d) whether the subject is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) the subject's physical or mental health or condition,
f) the subject's sexual life,
g) the commission or alleged commission by the subject of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Subject access request (SAR)

Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right they must do so in writing. All applications for subject access requests (SAR) must be made in writing to the Headteacher of the relevant school or MNSP CEO detailing the request.

A subject access request must be made in writing and must be accompanied by the appropriate fee. In most cases, the maximum fee will be £10, but this can vary, particularly if the information requested is for health or educational records. A request must include enough information to enable the person delegated by the Headteacher/CEO to satisfy themselves as to their identity of the person making the request and to find the information.

A reply must be received within 40 days as long as the necessary fee has been paid. A data controller should act promptly in requesting the fee or any further information necessary to fulfil the request. If a data controller is not processing personal information of which this individual is the data subject, the data controller must reply saying so.

Midsomer Norton Schools Partnership

Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your Headteacher immediately, who will then inform the DPO. Complete Section 1 and Section 2 of this form and email it to the Data Protection Officer and your Headteacher.

Section 1

Notification of Data Security Breach

Name of person reporting the incident	
Position / Role	
Date form completed	
Contact details of person reporting incident (email, and phone number including any extension)	

About the incident

Date incident discovered	
Date of incident	
Place of incident	
How did you find out about the data incident	
Brief description of incident or details of the information lost	
Number of data subjects affected (if known)	
Has any personal data been placed at risk? If so give full details:	
Brief description of any action taken at the time of the discovery	

Section 2

Assessment of Severity

Details of the IT systems, equipment, devices, records involved in the security breach:	

Details of information loss:

Type of Breach	Human error	System breakdown	Theft	Deleted or altered data	Lost (eg laptop or USB)
Category of Impact	Confidentiality		Integrity		Availability
Level of risk	High		Medium		Low
Breach categories					

What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, financial legal, liability or reputational consequences for the Trust or third parties?	
How many data subjects are affected?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as	

National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	

Implications of the breach

To be completed by the DPO or Headteacher

Received by:	
Date received:	
Forwarded for action to:	
On date:	

Section 3
Actions Taken

To be completed by the DPO/ LIO or the Headteacher

Actions Taken to reduce the impact of the breach

Other follow up actions required

Section 4

Notification

Is this a notifiable breach to the ICO	Yes	No
If reported to the ICO, Please give date.		

Reasons for decision about notifying the ICO

Was incident reported to police? If so, date and crime number	
Reported to other stakeholders? If Yes, date	
Communication sent to data subjects about the incident? If Yes, method used and date.	
Notified to other external agencies? If Yes, date and reason.	

Notifications (apart from the ICO, who else needs to be notified)

Are there lessons to learn from this incident?

Is there a training (re-training) requirement