ONE DEGREE ACADEMY

Striving for Excellence: *step-by-step*

One Degree Academy

Data Protection Policy

The Academy needs to gather and use personal data as part of its business. So that the Academy can comply with its legal obligations in relation to data protection, it is important that everyone who carries out work for the Academy follows the rules set out in this policy, including those relating to the data breach reporting procedure below. Everyone should note that the potential implications for the Academy and for individuals where there is a failure to follow these rules can be serious. These rules apply whether data is stored electronically, on paper or on other materials.

This policy applies to all employees, volunteers, consultants, suppliers and anyone else working for or on behalf of the Academy. It applies to all data that the Academy holds relating to identifiable individuals.

If you are an employee, this policy does not form part of your contract of employment and it can be amended at any time.

Last Review Date	**March 2018**
Next Review Date	**Sept 2018**
Author	**JHO**
Date Ratified by GB	
Person Responsible	**JHO / CHA**

Contents

1. Aims

Our school 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 Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of 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 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. 'Personal data' is data which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. 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

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

The school 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 our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school 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 responsibilities are set out in their link governor role details.

Our DPO is Charlie Harrell and is contactable via admin@onedegreeacademy.org. The Chief Operating Officer, Joe Howlett acts as a deputy DPO and will liaise with the DPO and carry out requests made by the DPO. The Chief Operating Officer is contactable via Jhowlett@onedegreeacademy.org

5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO and Chief Operating Officer 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 is based on data protection principles that our school 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, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

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

Staff responsibilities

Everyone who works for, or on behalf of the Academy, has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy. The Academy's Data Protection Officer is responsible for reviewing this policy and updating the Board of Governors on the Academy's data protection responsibilities and any risks in relation to the processing of data.

- You should only access data covered by this policy if you need it for the work you do for, or on behalf of, the Academy and you are authorised to do this work
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should only share personal data with people who are authorised by the Academy and with whom the Academy has the appropriate controls and safeguards in place.
- You must ensure that appropriate data privacy notices are issued to data subjects if this is part of your role.
- You should regularly review and update personal data which you have to deal with for work.
- You should not make unnecessary copies of personal data and should keep and dispose of those copies securely in the school confidential waste.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area without the consent of the data subject or the authorisation of the Data Protection Officer and Chief Operating Officer.
- You should lock drawers and filing cabinets which contain personal data.
- Don't leave paper with personal data lying about.
- You should not take personal data away from Academy premises without authorisation from your line manager or the Data Protection Officer.
- Personal data should not be kept for any longer than necessary – you should destroy or delete data in accordance with the table which can be found at the end of this policy.
- Personal data should be disposed of securely in the confidential waste when you have finished with it.

You should seek the express consent of the data subject before using or disclosing sensitive personal data if you are authorised to do so, or if not, speak to your line manager if you think additional consent is required.

You should ask for help from your manager or our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection we can improve upon.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We 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 school 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 school 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 school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- 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.
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

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons 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. This will be done in accordance with the school's record retention schedule.

7.3 Processing of personal data

The Academy will process personal data in accordance with our obligations and the Data Protection Principles above.

In addition, processing will only be permitted if:

- the data subject has consented for the data to be used in that way;
- processing is necessary for performance of a contract (actual or anticipated) with the data subject;
- the data has already been made public by the data subject;
- processing is necessary for compliance with a legal obligation;

- processing is necessary to protect someone's life or is in the public interest or there is official authority vested in the controller.

Special categories of data will only be processed if:

- the data subject has consented for the data to be used in that way;
- an exception in Article 9 GDPR applies.

7.4 Information given to data subjects

We will tell data subjects why we hold their data, who we might share the data with and their rights in relation to the data we hold. We will do this by issuing all data subjects with a "privacy notice" which will contain this information. Privacy notices for different types of data subjects are stored on the One Degree Academy website. Privacy notices will be reviewed regularly and updated by the Data Protection Officer.

8. Sharing personal data

We 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

We 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 or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we 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 school 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 must be submitted in writing, either by letter, email or fax to the DPO and Chief Operating Officer. They 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 and Chief Operating Officer.

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 our 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 at our 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
When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We 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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

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

When we refuse 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 us 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 and Chief Operating Officer. If staff receive such a request, they must immediately forward it to the DPO and Chief Operating Officer.

10. CCTV
As we are temporarily located at Heron Hall Academy, the on-site CCTV cameras are owned and maintained by our landlord, Cuckoo Hall Academies Trust who monitor their premises for security purposes.

There are visible signs showing that CCTV is in operation and images from this system are securely stored where only a limited number of Cuckoo Hall Academies Trust authorised persons may have access to them. The footage is automatically erased on a regular cycle and is not retained beyond that, but they may however be required to temporarily isolate and disclose CCTV footage to authorised third parties such as the police to assist with crime prevention or at the behest of a court order.

Our Data Protection Officer and senior staff will liaise directly with Cuckoo Hall Academies Trust with regard to any queries relating to CCTV images.

Cuckoo Hall Academies Trust's Privacy Notices and their Data Protection Policy can be found on Heron Hall Academy's website www.heronhallacademy.org.uk/Policies

11. Photographs and videos

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

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, we will clearly explain how the photograph and/or video may be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph and video in so far as we are able. For example, it may already have been distributed in print media. We will not use it further.

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

12. Data protection by design and default

We 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 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 school 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

13. Data security and storage of records
We 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 password protected and/or locked in a filing cabinet in the case of paper records
- 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Documents containing personal information must only be emailed using the One Degree Academy email and storage unless there is an exception that applies
- Attachments must not be downloaded onto personal phones or devices

14. 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches
Legally, certain data breaches, however minor, must be reported to the relevant authority within 72 hours of us becoming aware of the breach. In certain circumstances we must also inform the individuals who might be affected by the breach.

If you suspect or know of a data breach by the Academy, it is your duty to report the breach to the Data Protection Officer, or in his or her absence another senior manager, immediately. The Data Protection Officer or other senior person will then determine what action, if any, should be taken.

Examples of actions which might result in a reportable data breach are:

- access of data by an unauthorised third party (eg. by hacking the Academy's computer system)
- sending personal data to an incorrect recipient
- loss or theft of devices (such as mobile phones or laptops) which contain personal data
- alteration of personal data without permission
- loss of availability of personal data (eg. where a password for a password protected document containing personal data is forgotten)

This list is not exhaustive so, if in doubt, please speak to the Data Protection Officer or another senior manager as soon as possible.

All data breaches will be recorded by the Academy, even if the breach does not need to be reported.

The Data Protection Officer and other senior managers will refer to the section below to determine next steps on receipt of information concerning a possible data breach.

DPO duties in the event of a suspected breach

If the Data Protection Officer (or any senior manager, such as the Chief Operating Officer) becomes aware of a suspected data breach he or she will:

- take steps to recover any lost data and limit the damage that the breach may cause
- inform anyone who needs to know about the breach (eg the individuals affected by the breach, the Police, insurers etc.) and provide them with the following clear information:
    - what has happened
    - what is being done to address the breach
    - your contact details for further information or assistance
    - advice as to what they might be able to do to protect themselves.
- nominate someone to investigate the breach
- assess the potential adverse consequences of the breach and the likelihood of those consequences occurring.
- in accordance with ICO guidelines, report the matter to the Information Commissioner's Office (ICO) without delay, and in any event within 72 hours of being aware of the breach, if the breach is likely to result in a risk to the rights and freedoms of individuals
- establish whether further action is required in order to prevent a further data breach.

16. Third Parties
Data protection clauses in all existing contracts need to reflect the GDPR requirements.

We have to include certain information in contracts with suppliers (such as insurers, payroll and school club providers) where the school passes data to them, and they receive and store it.

We have also carried out some data protection due diligence on any existing suppliers, or other third parties which hold personal data on our behalf, to make sure they're preparing for the GDPR and have adequate security measures in place (see appendix 2 for our third party checklist).

17. Audit and 'data ecosystem'
We have a data ecosystem that:

- Maintain records of how we process activities
- Demonstrates how we comply with the data protection principles

18. Data Protection Impact Assessment
Data protection impact assessments (DPIAs) are a tool that can help us identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow us to identify and fix problems at an early stage.

The ICO explains that you must carry out a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
- Large-scale, systematic monitoring of public areas (such as CCTV)

In most cases, meeting 2 criteria would require a DPIA, but a data controller can decide that a processing operation meeting only one of these criteria requires a DPIA.

The criteria are:

1. Evaluation or scoring
2. Automated decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself prevents data subjects from exercising a right or using a service or contract

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of persons, and for which there has been a change of the risks.

A DPIA should be carried out **prior** to the data processing.

The data controller:

- Is responsible for ensuring that the DPIA is carried out, although someone else inside or outside the organisation can do it
- Must seek the advice of the data protection officer. This advice, and the decisions taken by the controller, should be documented within the DPIA
- Must seek the views of data subjects or their representatives, where appropriate

While there is no legal requirement to publish a DPIA, the controller can choose to do so.

The ICO, linked to above, says that a DPIA should include:

- A description of the processing operations and purposes, including, where applicable, the legitimate interests pursued by the data controller
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate that you comply

A DPIA can address more than one project.

On page 22, the guidelines include criteria for an acceptable DPIA. These are:

- A systematic description of the processing is provided
- Necessity and proportionality are assessed
- Risks to the rights and freedoms of data subjects are managed
- Interested parties are involved

We will:

1. Identify the need for a PIA
2. Describe the information flows
3. Identify the privacy and related risks
4. Identify privacy solutions
5. Sign off and record the PIA outcomes
6. Integrate the PIA outcomes back into the project plan

19. Privacy notices
Our privacy notices are kept up to date on the school website. These must state our:

- Legal basis for processing;
- Notice of the individual's right to make a complaint to the ICO (as the 'supervisory authority')
- Notice of other rights in relation to access and correcting inaccurate data
- They must be in clear and plain language

20. Consent

- Consent forms must be specific, granular, clear, prominent, opt-in, documented and easily withdrawn
- We record consent have an effective audit trail

21. Training
All staff and governors are provided with data protection training.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

22. Monitoring arrangements
The DPO and governing body is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full governing board.

23. Links with other policies
This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding policy
- ICT policy
- Use of personal devices

Appendix 1: Personal data breach procedure
This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO and Chief Operating Officer.
- The DPO with the support of the Chief Operating Officer will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO or Chief Operating Officer will alert the Principal and the chair of governors
- The DPO or Chief Operating Officer will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO with the support of the Chief Operating Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO with the support of the Chief Operating Officer will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO with the support of the Chief Operating Officer will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the SLT drive in the GDPR folder.
- Where the ICO must be notified, the DPO with the support of the Chief Operating Officer will do this via the 'report a breach' page of the ICO website or by calling 0303 123 1113 within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO with the support of the Chief Operating Officer will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO with the support of the Chief Operating Officer will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO with the support of the Chief Operating Officer will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO with the support of the Chief Operating Officer will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the O drive in the GDPR folder.
- The DPO, Chief Operating Officer and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Appendix 2: Supplier Contracts

Supplier contracts – GDPR checklist. This will be used to verify during the audit that our suppliers meet the requirements for GDPR.

For the points in the grey rows, the information you include will need to be specific to each contract.

Information to include to meet GDPR requirements	✓
The subject matter, duration, nature and purpose of the data processing	
The type(s) of personal data being processed	
The categories of the data subjects (the individuals whose data is being processed)	
The obligations and rights of the data controller (your school)	
The data processer (the third party/supplier) processes data only on the documented instructions of the school	
The people who process the data are committed to confidentiality, or are required by law to uphold confidentiality	
The third party takes measures to ensure data is processed securely	
The third party will not engage another processor without prior written authorisation from the school	
If the third party does engage another processor, this processor will be bound by a written contract with the same data protection conditions as are in the contract with the school	
The third party helps the school comply with: • Upholding the data rights of individuals • Secure processing • Reporting and communicating data breaches • Conducting impact assessments where relevant	
The third party deletes or returns the personal data to the school at the end of the provision of services (unless the law states that the information must be kept)	
The third party makes information available to the school to demonstrate its compliance with the obligations in the contract, and allows the school or another party instructed by the school to conduct audits and inspections	