TDAP049B
UK GENERAL DATA PROTECTION REGULATIONS (UK-GDPR) POLICY

Requisite: Dorcan Requirement				**Responsible Committee: F&P**	
Vers.	Approval Date	Committee	Head	Chair	Next Review Date
A	18/06/2018	*Full Governing Body*			November 2021
B	13/11/2022	*Finance and Premises*			January 2025

Contents

1. Aims

The aim for this policy is to ensure that all personal data collected about staff, students, parents, trustees, members, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UKGDPR).

This policy applies to all personal data, regardless of whether it is in paper or electronic format. It is the responsibility of all members of The Dorcan Academy to take reasonable care when handling, using or transferring personal data so it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals, Academies and the whole Academy concerned. It can bring the Academy into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the Academy and the individuals involved. All transfer of data is subject to risk of loss or contamination.

2. Legislation and guidance

This policy meets the requirements of the UK 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement from the ESFA and The Dorcan Academy's Articles of Association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Political opinions • Racial or ethnic origin • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Dorcan Academy processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

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

5.1 Trustees & Governing body

The board of trustees and governing body have overall responsibility for ensuring that The Dorcan Academy 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 for compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities and any data protection issues directly to the governors.

The DPO is also the first point of contact for individuals whose data the Academy processes. The DPO is Astrid Broderstad and is contactable via email abroderstad@dorcan.co.uk

5.3 Staff responsibilities

Each Academy and core business department within The Dorcan Academy is responsible for the following tasks within their Academy:

- Be the focal point for data protection within the Academy
- Complete Processing Activity and data questionnaires when required
- Report incident and data breach to the DPO
- Challenge security of IT systems and employees working practice if necessary
- Undertake data protection training
- Identify risks of data protection to DPO for further investigation.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy 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 UK
- 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 UK GDPR is based on data protection principles that The Dorcan Academy must comply with. The principles say that personal data must be:

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

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

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 Academy can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy 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 Academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Academy or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) 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 UK GDPR and Data Protection Act 2018.

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

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

7.2 Limitation, minimisation and accuracy

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 Dorcan Academy data deletion guidelines that can be found in section 16.

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 student 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
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, Online Solution Providers. 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 stand-alone 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 that affects any of our students or staff.

We may also share personal data with marketing companies who will deliver specifically target information to staff, parents / carers or students. Consent will be obtained before

any marketing related communications are sent and will be reviewed every 2 years. The individuals have the right to withdraw consent, requested by completing the relevant form available from the Academy.

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

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy 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 by completing the form available from the Academy office or by contacting the DPO.
If staff receive a subject access request in any format they must immediately forward it to the DPO.

9.1 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, some subject access requests from parents or carers of students at our Academy may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case- by-case basis.

9.2 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 student 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.

9.3 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. If staff receive such a request, they must immediately forward it to the DPO.

Freedom of Information Procedures

Freedom of Information requests must be submitted using our FOI form. The Academy will respond within 20 days of the original request.

Freedom of Information Policy

All Academies are committed to comply with the relevant legislation pertaining to a freedom of information request, and will follow the guidance set out by the Information

Commissioner's Office.

If you receive any type of individual access request, please follow the procedure outlined in Appendix 3.

- Right to Be Informed: the individual is seeking information that should have been provided to them in the privacy notice, or the notice itself
- Right to Erasure: the individual is seeking that their data be deleted and/or 'forgotten'
- Right of Access: the individual is seeking confirmation that their data is being processed; access to, or a copy, their data, or other supplementary information
- Right to Rectification: the individual is claiming that their data is inaccurate or incomplete, and is seeking for it to be rectified
- Right to Data Portability: the individual is seeking a reusable copy of their data, or to have the data transmitted to another entity
- Right to withdraw consent: the individual is seeking to withdraw their consent to the processing of their data

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within 15 Academy days of receipt of a written request.

11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive Academy dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy will get consent from at least one parent or carer before we take any biometric data from their child and first process it. This consent will be recorded within the individual Academy's Management Information System.

Parents/carers and students have the right to choose not to use the Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for Academy dinners in cash at each transaction if they wish or be provided with a payment card if applicable.

Parents/carers and students can object to participation in the Academy's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the Academy's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of

accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Academy will delete any relevant data already captured.

12. CCTV

We use CCTV across all Academy establishments for the purpose of safeguarding and security. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by signs explaining that CCTV is in use.

All recordings will be retained for no more than 30 days and every effort will be made to ensure these do not record inappropriate images e.g. in a toilet cubicle.

Any enquiries about the CCTV system should be directed to the DPO.

13. Photographs and videos

As part of our Academy activities, we may take photographs and record images of individuals within our Academy.
We will obtain written consent from parents/carers/ students for photographs and videos to be taken of students for Academy use, communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. To withdraw consent please complete the relevant form available from the Academy office.

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.

See our Digital Image policy for more information on our use of photographs and videos.

14. 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
- Completing privacy impact assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents, 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 The Dorcan Academy DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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 kept in secure locations when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, this will be agreed and recorded by the DPO prior to leaving the Academy
- Staff passwords are used to access Academy computers and online resources, these must meet complexity rules which include the following rules:
  - Preferably 8 characters long
  - Containing letters, numbers and special characters
  - Must be changed every 90 days
  - The password cannot be the same as the last 10 previous passwords
- Failure to enter the correct password will lock the users account. Please refer to the IT Password Policy for more information.
- As part of ongoing cyber security awareness for students, they're advised to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media,

such as laptops and USB devices

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment
- 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)

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Dorcan Academy will follow the Impact Levels as follows:

The Dorcan Academy Marking Scheme	Impact Level (IL)	Release and Destruction Classification.
NOT PROTECTIVELY MARKED	0	None
CONFIDENTIAL	1	Securely shredded or securely deleted
HIGHLY CONFIDENTIAL	2	Securely shredded or securely deleted

All Academy staff, independent contractors working for it, and delivery partners, must comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data should be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer. Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students/students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long- term significant damage to reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the document eg. "IL0, IL1 or IL2".

16. Disposal of records

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

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

guarantees that it complies with data protection law.

Personal data will be held on ICT systems for a period of 6 months, after this period it will be deleted and no formal backup will be kept unless required by law. Once an employee leaves The Dorcan Academy they'll have a 6-month period from the date of leaving to request copies of any personal information held on personal drives including email. Any request for copies of work will be agreed by the DPO to ensure the business is not jeopardised in anyway by releasing this data.

We will use the following data retention periods for the categories of data below:

Description	Location of Stored Data	Retention / Disposal Period	Disposal Method
Recruitment paperwork (unsuccessful)	HR Cabinets	6 months after interview	Securely deleted / overwritten
Ex-Employee Data (electronic)	HR Database	7 years after date of leaving	Securely deleted / overwritten
Ex-Employee Data (paper based)	HR Cabinets	7 years after date of leaving	Securely shredded
Employee Absence Forms (paper based)	HR Cabinets	6 years	Securely shredded, HR keep records in HR Database or employee file
Employee Overtime Forms (paper based)	Finance office cabinets	6 years	Securely shredded, HR keep records in HR Database or employee file
Employee payroll records and other financial records	Finance office cabinets	6 years	Securely shredded
Student Safeguarding Files	Academy Locked Cabinets	Data kept until individual 25 years old	Securely shredded
Ex Student Data (electronic)	Academy Locked Cabinets	Data kept until individual 25 years old	Securely deleted / overwritten
Ex Student Data (paper based)	Academy Locked Cabinets	Data kept until individual 25 years old	Securely shredded

17. Personal Data Breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Academy context may include, but are not limited to:

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

18. Training

All staff and governors are provided with continued data protection training as part of their roles.

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when legislation changes, if any changes that are made affect our Academy's practice. Otherwise, or from then on, this policy will be reviewed every 3 years and shared with all relevant stakeholders.

20. Links With Other Policies

The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies

- Complaints
- Safeguarding Children and Young people
- Behaviour
- Anti-Bullying
- Lettings and Use of Premises
- Special Educational Needs
- Academy trips
- Curriculum
- Children in Care
- Health and Safety
- Sex and Relationships Education
- Security
- Equality Diversity and Community Cohesion
- Students with Medical Needs
- Internet Access and Use
- Use of ICT and Website
- Young Carers
- E-safety
- Cloud based
- Password Policy

- Digital Images
- Privacy and Confidentiality
- Whistle blowing

The above list is not exhaustive but when undertaking development or planning of any kind the Academy will consider safeguarding matters

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
- The DPO 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 will alert the Head Teacher and the Chair of Governors
- The DPO 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 will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO 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 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.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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 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 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 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 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 documented and stored.

- The DPO and Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant

unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2 - Use of Protective Marking

	The information	The technology	Notes on Protect Markings (Impact Level)
Academy life and events	Academy terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of students work, lunchtime menus, extended services, parent consultation events	Publically accessible technology such as Academy websites or portal, emailed newsletters, subscription text services, mobile apps	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual student / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Via secure systems, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the Confidential (Level 1) category. There may be students/ students whose personal data requires a HIGHLY CONFIEDENTIAL marking (Impact Level 2). For example, the home address of a child at risk. In this case, the Academy may decide not to make this student / student record available in this way.

Messages and alerts	Attendance, behavioural, achievement, sickness, Academy closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging or Learning Platforms or portals or mobile apps might be used to alert parents to issues.	Most of this information will fall into the CONFIDENTIAL (Level 1) category. However, since it is not practical to encrypt email or text messages to parents, Academies should not send detailed personally identifiable information. General, anonymous alerts about Academies closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

GENERAL DATA PROTECTION (GDPR) POLICY

Appendix 3: Data Subject Access or individual requests procedure

The following procedure should be followed if you receive a Data Subject or individual rights request. If you are verbally asked how a request should be made please direct them to the DPO. Alternatively if you personally receive a request via email or letter then the following procedure must be followed:

All Staff

1. On receiving any request, please forward this to your DPO within 2 working days of receipt.

DPO Procedure

2. Once you receive the request, please acknowledge receipt via email within 3 working days.
3. Record the request
4. Investigate the request with the relevant departments and ensure the requester is informed if
   any extension to the standard 30 days will be required.

Ensure any communication is recorded.

- **Revision Notes**

Rev A:	Original
Rev B:	Agreed and approved by the Audit, Finance and Premises Committee 11/1/2022