




|  |  |   |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|--|--|---|--|---------------------------|---|----------------------------|-----------------------|--------------------|-------------------|-----------------------|-------------------|---------------------|-------------------|--------------------|-------------------|
| <br><br><br><br>  | <table border="1"> <tr> <td><b>Policy Focus</b></td> <td><b>GDPR and Data Protection Policy</b></td> </tr> <tr> <td><b>Lead Policy Holder</b></td> <td><b>Name: Hannah Moon, Chief Executive Officer</b></td> </tr> <tr> <td><b>Designated Director</b></td> <td><b>Judith Johnson</b></td> </tr> <tr> <td><b>Policy Date</b></td> <td><b>March 2019</b></td> </tr> <tr> <td><b>Policy Version</b></td> <td><b>Version: 1</b></td> </tr> <tr> <td><b>BoD Adoption</b></td> <td><b>March 2020</b></td> </tr> <tr> <td><b>Review Date</b></td> <td><b>March 2022</b></td> </tr> </table> | <b>Policy Focus</b>                               | <b>GDPR and Data Protection Policy</b> | <b>Lead Policy Holder</b> | <b>Name: Hannah Moon, Chief Executive Officer</b> | <b>Designated Director</b> | <b>Judith Johnson</b> | <b>Policy Date</b> | <b>March 2019</b> | <b>Policy Version</b> | <b>Version: 1</b> | <b>BoD Adoption</b> | <b>March 2020</b> | <b>Review Date</b> | <b>March 2022</b> |
|  | <b>Policy Focus</b>  | <b>GDPR and Data Protection Policy</b>            |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>Lead Policy Holder</b>  | <b>Name: Hannah Moon, Chief Executive Officer</b> |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>Designated Director</b>   | <b>Judith Johnson</b>                             |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>Policy Date</b>   | <b>March 2019</b>                                 |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>Policy Version</b>  | <b>Version: 1</b>                                 |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>BoD Adoption</b>  | <b>March 2020</b>                                 |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
|  | <b>Review Date</b>   | <b>March 2022</b>                                 |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |
| <p><b>School Aim</b></p> <p>Our Company (Life Chance Education Ltd) is committed to transforming the life chances of the young people and families that we work with. We support children who have suffered trauma, Adverse Childhood Experiences (ACEs), and exhibit Social, Emotional and Mental Health difficulties (SEMH). Our educational staff, multi-disciplinary team of therapists, and support team work together to create an environment that meets the holistic needs of children who have difficult or complex life stories.</p> <p>By delivering the best features of a special school and alternative provision, coupled to innovative educational and therapeutic frameworks, we can help our students thrive. We believe that children don't have to be bound by the past but can build a bright future if they have the right support.</p> <p>Our Mission is to ensure that we help every child we work with achieve their full potential, both academically and personally. As a school we aspire to being outstanding, so our students can be too – as exemplified in our school motto:</p> <p style="text-align: center;"><b><i>'Being the Best We Can Be'</i></b></p> <p>Our Aims are to:</p> <ul style="list-style-type: none"> <li>▪ Meet the previously unmet needs of young people and enable learning and employment.</li> <li>▪ Provide positive interventions into barriers to learning and negative family or intergenerational life cycles.</li> <li>▪ Contribute to community and social change.</li> <li>▪ Reduce costs to society in terms of both social and economic benefits</li> </ul> <p>To reach these aims we will use concepts and best practice in learning, neuroscience, emotional well-being, child development and coaching.</p> |  |   |  |                           |   |                            |                       |                    |                   |                       |                   |                     |                   |                    |                   |

## Contents

### Glossary of Acronyms (if applicable)

1. **Statement of Intent for this Policy**
2. **Statutory / Legislative Basis**
3. **Links to Other Related Policies**
4. **Monitoring Review & Evaluation: Compliance - Consistency - Impact**
5. **Key Policy Information / Guidance Relating to our Practice**
6. **Implications for Stakeholders**
7. **Relevant Data Sets / Metrics**
8. **Relevant Resources**

### Appendices (Embedded / E.Links)

*(Statutory Documents – Data Sets – Recording Templates – Resources - SoL etc)*

## Glossary of Acronyms

|             |                                     |
|-------------|-------------------------------------|
| <b>GDPR</b> | General Data Protection Regulations |
| <b>ICO</b>  | Information Commissioner's Office   |
| <b>CEO</b>  | Chief Executive Officer             |
| <b>SLT</b>  | Senior Leadership Team              |
| <b>CPD</b>  | Continue Professional Development   |
| <b>SEPS</b> | Self-Evaluation Position Statement  |
| <b>HoS</b>  | Head of School                      |
| <b>LA</b>   | Local Authority                     |

## 1. Statement of Intent for this Policy

This Policy is to provide all staff with the necessary information to enable them to meet their responsibilities and to ensure consistent and effective practice across all school sites. It demonstrates the school's commitment with regard to [staff](#), students, parents and other partners.

This Policy contributes to the school's Administrative, Financial and Operations folio (see section 3).

Our core principles are:

- Aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals, is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR), and the expected provisions of the Data Protection Act 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. Statutory / Legislative Basis

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](#).

In addition, this policy 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

## 3. Links to Other Related Policies / Procedures

This policy sits within the Administrative, Financial and Operations Portfolio of Policies which School for Inspiring Talents has adopted. It therefore relates to other policies in that themed grouping which include:

- Business Continuity Plan
- Expenses Policy
- Fire & Emergency Policy & Procedures
- Premises Management Policy
- Risk Register
- Feedback Policy
- Gifts Policy
- Scheme of Delegation
- Volunteers Policy

## 4. Monitoring, Review & Evaluation (MRE): Compliance - Consistency – Impact

Monitoring, Review and Evaluation (MRE) of all aspects of our work as a school is undertaken to ensure that we are delivering on what we say we want to achieve with and for our students. In the interests of equity and high expectations for all our students, we are continuously checking for:

- Compliance and for Quality
- Implementation match with our Intent
- Consistency between staff and sites
- And to ensure value for money for our Referring Local Authorities.

Our school staff are part of our school culture of continuous improvement based on supervision, self-reflection, peer working, and CPD. Daily staff briefings and debriefings provide immediate feedback and strategies for even greater success next time round.

Our framework for MRE is achieved via 3 key approaches:

### Internally

- Our annual Self Evaluation Position Statement (SEPS) aligned with Ofsted Evaluation Areas and Grade Descriptors

|                                  |   |                                |              |
|----------------------------------|---|--------------------------------|--------------|
| Ref: LCEd & SfiT School Policies | Policy Focus: Administration, Financial & Ops and Safeguarding folios | Policy Date & Version v1 03/20 | Page 3 of 13 |
|----------------------------------|---|--------------------------------|--------------|

- Learning Walks by HoS in own and other Phases/Sites
- Individual Student Assessment Framework and Trackers
- CEO & Executive Principal’s Observations, Spot Sampling and Random Checks
- Monthly SLT Progress Reviews of the Operational School Improvement Plan (OSIP)
- Heads of School Monitoring
- Appraisal & Performance Management approaches.
- SchoolPod, Incident Logs Reviews and Spot Sampling, plus trend monitoring across the year
- Staff Briefings
- Student Voice Surveys
- Peer Reviews through Team Working
- CPD Evaluations

**Accountability MRE**

- Our Board of Directors Link Portfolio Visits and Observations
- Director Monitoring of all Independent School Standards (ISS) Themes annually as part of a rolling programme
- Termly Directors Scrutiny of the CEO & Executive Principal Reports to the Board
- Termly H&S checks
- Directors Involvement in the cycle of Policy Review
- Financial and Curriculum Resource Monitoring

**Externally**

- Referring LAs’ Annual Health Checks and Audits
- Commissioned Reviews of aspects of practice – specialist and generic e.g. Behaviour, Health & Safety
- Feedback from submissions for Awards and Quality Standards e.g. TISS
- Parent / Carer Feedback e.g. via Class Dojo
- Ofsted Monitoring and Inspection Visits
- User Schools Feedback

**Additionally, and with specific context to the focus for this policy:**

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. Key Policy Content - Information / Guidance Relating to our Practice**

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 Board of Directors**

The Board of Directors have overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**5.2 Headteacher**

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

**5.3 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 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

### 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

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

### Collecting Personal Data

#### 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 data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (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.

#### 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.

## 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.

### 9.1 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 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.

## 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.

## 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.

## 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.

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 pupil) within 15 school days of receipt of a written request.

### Photographs and Images

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 for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- media 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 pages

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

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

See our child protection and safeguarding policy for more information on our use of photographs and videos.

### 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:

- 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 (the DPO will advise on this process)
- 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 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



## 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 under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- 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
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or Directors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable use Policy/ICT Code of Conduct)
- 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)

## 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.

## Personal Data Breaches

The school 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 as set out in appendix 1.

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

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

## Training

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

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

## Monitoring Arrangements

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 **every 2 years** and shared with the Board of Directors.

## 6. Implications for Stakeholders

|                                    |  |
|------------------------------------|--|
| <b>Board of Directors</b>          | Directors will abide by the policy set out in Section 5 and review every two years   |
| <b>All Staff</b>                   | All staff should be made aware of the GDPR policy and ensure they understand their responsibility  |
| <b>Designated Specialist Staff</b> | <b>The CEO (Chief Executive Officer)</b> as line Manager of the Administration/Facilities team, has a specific responsibility to ensure the GDPR policy has been completed and adhered to  |
| <b>Students</b>                    | Personal data belongs to the individual student  |
| <b>Families/Carers</b>             | 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.<br>Written consent has to be given in writing in relation to the following: <ul style="list-style-type: none"> <li>▪ media Within school on notice boards and in school magazines, brochures, newsletters, etc.</li> <li>▪ Outside of school by external agencies such as the school photographer, newspapers, campaigns</li> <li>▪ Online on our school website or social pages</li> </ul>   |
| <b>Referring LAs</b>               | Professional responsibility to share information with other agencies in order to safeguard children and that the Data Protection Act 2018 is not a barrier to sharing information where the failure to do so would place a child at risk of harm   |
| <b>Contractors</b>                 | 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: <ul style="list-style-type: none"> <li>▪ Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law</li> <li>▪ 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</li> <li>▪ 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</li> </ul> |
| <b>Visitors</b>                    | Visitors must sign in at reception and will be given an identification badge, which displays their name and occupation   |
| <b>Agencies</b>                    | All agency staff refer to the Child Protection Policy and GDPR policy  |
| <b>Schools</b>                     |  |

## 7. Relevant Data Sets / Metrics

## 8. Relevant Resources

<https://ico.org.uk/for-organisations/guide-to-data-protection/>

<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/>

<https://www.gov.uk/government/publications/data-handling-procedures-in-government>

## Appendices 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 Executive Principal
- The school will investigate the report and determine whether a breach has occurred. To decide, the School 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 school will alert the headteacher and Board of Directors
- The school 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 school will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The school 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 school 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 school must notify the ICO.

- The school 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 school's computer system.
- Where the ICO must be notified, the school 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 school
    - ✦ 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 school 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 school expects to have further information. The school will submit the remaining information as soon as possible

- The school 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 school 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 Executive Principal
  - ✦ 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 school 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 school 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 school’s computer system. The headteacher 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 School will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The School 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*

**EVALUATION AND MONITORING**

This policy will be reviewed every two years by the COO/Board of Directors