Enfield Grammar School

An Academy Trust

(Company No. 07697044)

Data Protection Policy

REVIEWED	January 2017
AUTHOR	Headteacher
APPROVED	January 2017
NEXT REVIEW	January 2019

Enfield Grammar School collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all that we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed.
- Process data only for limited purposes.
- Ensure that all data processed is adequate, relevant and not excessive.
- Ensure that data processed is accurate.
- Not keep data longer than is necessary.
- Process the data in accordance with the data subject's rights.
- Ensure that data is secure.
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example our Local Authority or Ofsted. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Under no circumstances will the school disclose information or data:

- That would cause serious harm to the child or anyone else's physical or mental health or condition.
- Indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child.
- Recorded by the pupil in an examination.
- That would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.
- In the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Requesting data

Pupils have a right under the Data Protection Act to request information that the school has collected about them by any data controller.

Privacy notice

The school will issue a privacy notice to all pupils and staff when they first join the school. This will refer pupils, parents, and staff to our local authority website where you can find all the information on what data is collected and how it is used.

The school will not collect or process the biometric data of any pupil without parental consent. This includes fingerprint identification and also covers iris and retina scanning, and face recognition. If the school wishes to collect this information parents will be contacted for consent. This request for consent will include full explanation about the type of biometric information that will be taken and how it will be used, as well as an explanation of the parents' and pupil's right to refuse or withdraw their consent.

Staff

We are legally obliged to protect certain information on our staff. School staff have a right to see records of their personal information. Staff who wish to access this information can make a subject access request under the Data Protection Act 1998. Disclosure of these records will be made once third party information has been removed in accordance with the Data Protection Act 1998.

Access to data and disclosure

Third parties

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from Enfield Grammar School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce the Education Act.

- **School staff**
  School staff will have restricted access to pupils' personal data and will be given access only on a 'need to know' basis in the course of their duties within the school. All staff are well informed of the Data Protection Act and how their conduct must correspond with this. Staff will use data only for the purpose of which it was collected, and any staff that are found to be acting intentionally in breach of this will be disciplined in line with the seriousness of their misconduct.

Location of information and data

Hard copy data, records, and personal information should be stored out of sight and in a locked cupboard no matter what format it is in. The only exception to this is medical information that may require immediate access during the school day.

Sensitive or personal information and data should ideally not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. The USB must be one provided by the school and be signed out and in by the ICT Manager.
- These USBs must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Retention of data

The school will not keep personal data on pupils for any longer than is necessary. Information such as statistical data, and information that is collected to be kept as part of school records, will be kept by the school even after the child leaves.

It is very important that all examination results certificates and records indicating the progress of a student are safely kept by their parents/carers as the school cannot guarantee that this information will be kept indefinitely by the school.

The school cannot guarantee that any information will be kept by the school indefinitely, although records are usually kept for a period of 7 years after the child has left the school.

Procedures to deal with a serious data breach

- Please see appendix A attached.

Appendix A

Data Protection - Data Breach Procedure for Enfield Grammar School

Enfield Grammar School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by Enfield Grammar School. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Enfield Grammar School if a data protection breach takes place.

Legal Context

The Data Protection Act 1998 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the Act states that organisations which process personal data must take

"appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as fire or flood.
- Hacking.
- 'Blagging' offences where information is obtained by deception.

Immediate Containment/Recovery

In discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Headteacher or, in their absence, either the Deputy Headteacher or the School Business Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Headteacher (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT Manager/Technician.

3. The Headteacher (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the School's responsibility to take the appropriate action and conduct any investigation.

4. The Headteacher (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The Headteacher (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    - Attempting to recover lost equipment.
    - Contacting the relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Headteacher (or nominated representative).
    - The use of back-ups to restore lost/damaged/stolen data.
    - If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    - If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Headteacher (or nominated representative) to fully investigate the breach. The Headteacher (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data.
- Its sensitivity.
- What protections are in place (e.g. encryption).
- What has happened to the data.
- Whether the data could be put to any illegal or inappropriate use.
- How many people are affected.
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The Headteacher (or nominated

representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified. Every incident should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at: https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf
- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure).

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available SLT meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with the School Business Manager for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The Headteacher should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision. If staff have any queries in relation to the policy, they should discuss this with the Headteacher.