HILLSIDE JUNIOR SCHOOL

Data Protection Policy and Privacy Notice

POLICY DETAILS:
Legal Status: Statutory
Adopted: 22 May 2018
Version Date: April 2018
Last Review: N/A
Next Review: May 2019

Contents

1. Aims

During the course of normal school activities we receive, use and store personal information about our pupils, parents, suppliers and staff. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018, which incorporates the requirements of the EU General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018 and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force on 25 May 2018.

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. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of the data controller to the Data Protection Officer of Grow Education Partners. The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

We will ensure the following:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body

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

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. Where required, they will provide an annual report of their activities directly to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is appointed from Grow Education Partners and is contactable via Grow Education Partners, London Diocesan House, 36 Causton St, Westminster, London SW1P 4AU Tel: 0207 9321175 -TBC

Headteacher

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

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

7. Privacy/fair processing notice

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Personal information such as name, unique pupil number and address
- Attendance information such as sessions attended, number of absences and absence reasons
- Data on pupil characteristics such as ethnicity, language, nationality, country of birth and free school meal eligibility
- Assessment information, relevant medical information, special educational needs information, exclusion/behavioural information

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details including bank details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures
- Continuous Service /Long Service Awards

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We routinely share workforce data with

- Our Local Authority
- The Department for Education (DfE)
- The Schools HR Co-operative
- Governor Support Service
- SIMS for Schools
- Medigold Health
- Dataplan Education (payroll provider)
- Surrey Country Council (LGPS administrator)
- Teachers' Pension

We will not share information about staff with third parties without consent unless the law and our policies allows us to, however, we are required by law to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Headteacher.

8. 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:

Subject access requests must be submitted in writing, either by letter or email. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days.

If a subject access request does not relate to the educational record, we will respond within 30 calendar days.

9. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), 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
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred paper-based records, and override electronic files. We may also use an outside company to safely dispose of paper-based and electronic records.

12. Record Retention

We will only retain data for as long as is necessary to complete processing. However, where we have a statutory obligation to retain data please refer to our Retention Guidelines Policy.
We use the Information Records Management Society (IRMS) Toolkit for Schools as reference. A copy of this is available to view at http://irms.org.uk/page/SchoolsToolkit

13. Training

Our 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 or the school's processes make it necessary.

14. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force 25 May 2018.
We are already working to be GDPR compliant and will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

15. Monitoring arrangements

The Governing Body of Hillside Junior School is responsible for monitoring and reviewing this policy. The Data Protection Officer of Grow Education Partners checks that the school complies with this policy by, among other things, reviewing school records annually and visiting the school three times per annum.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the Governing Body.

16. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

Appendix 1: Data Breach Procedure including Register

Policy Statement

Hillside Junior 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 Hillside Junior 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 Hillside Junior School if a data protection breach takes place.

Introduction

Data Protection legislation is changing in May 2018. The Data Protection Act 1998 will be superceded by the Data Protection Act 2018 which will incorporate the requirements of the EU General Data Protection Regulation (GDPR).

GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified.

All organisations are legally required to ensure any Personal Data is processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

GDPR places a duty on all organisations to manage, report (where necessary), and investigate all personal data breaches.

Types of Breach

Under GDPR, a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

It also means that a breach is more than just about losing personal data.

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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it. This includes notifying, where required, the appropriate Supervisory Authority. In the UK, this role is held by the Information Commissioners Office (ICO).

Immediate Containment/Recovery

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this **within 72 hours of becoming aware** of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

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 the Deputy Headteacher. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Data Protection Officer (DPO) should be informed as soon as is practicable (within 24 hours of the breach being detected).
3. The Headteacher (or nominated representative) and DPO 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 technician.
4. The Headteacher (or nominated representative) should inform the Chair of Governors.
5. The Headteacher (or nominated representative) and DPO must 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.
6. The Headteacher (or nominated representative) and DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    - Attempting to recover lost equipment.
    - Contacting the relevant Local Authority 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) and DPO.
    - 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) and DPO to fully investigate the breach. This 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. This should be added to the School's breach register. (see Appendix 1a)

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

Where a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must notify the ICO within 72 hours of the breach being detected.

The school must also contact the individuals affected within 72 hours.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

It is essential that the School with assistance from their DPO, assess this case by case, looking at all relevant factors.

If the school is unsure whether an incident should be notified to the ICO they should immediately contact their DPO for advice.

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher (or nominated representative) and DPO should fully review both the causes of the breach and the effectiveness of the response to it.

It should be formally documented and made available to the Senior Leadership Team (SLT) for discussion.

If systemic or ongoing problems are identified, then an action plan must be drawn up to address those problems. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources 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 all 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 their line manager or the Headteacher.

Appendix 1a Data Breach Register

Breach Register V1.0 190318.xlsx

The register is available as electronic version on Hillside Junior School's server:

O:\Data\Data Protection\GDPR\Initial Assessment AzteQ\Breach Register V1.0 190318.xlsx

Appendix 2: Subject Access Request (SAR) Register

SAR Control Register.xlsx

The register is available as electronic version on Hillside Junior School's server:

O:\Data\Data Protection\GDPR\Initial Assessment AzteQ\SAR Control Register.xlsx