Data Protection Policy – Holmfirth High School

Person responsible: **DC**
Review date: **March 2019**

Contents:

[1] The term 'parent' includes any person or body with parental responsibility such as a foster parent, carer, guardian or local authority.

Introduction

In order to operate efficiently Holmfirth High School has to collect and use information about people with whom it works and the students it provides an education to. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

It is the responsibility of the Governors to ensure procedures are in place to ensure that the school complies with Data Protection legislation, eg including, but not limited to, the General Data Protection Regulation (GDPR) and The Data Protection Act.

The school is committed to ensuring personal data is properly managed and that it ensures compliance with current data protection legislation. The school will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

1. Scope

This policy applies to all employees, governors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the school.

This policy applies to all personal data created or held by the school in whatever format (eg paper, electronic, email, microfiche, film) and however it is stored, (for example, ICT system/database, shared drive filing structure, workbooks, email, filing cabinet, shelving and personal filing drawers).

Personal data is information about living, identifiable individuals, or an identifier or identifiers that can be used to identify a living individual. It covers both facts and opinions about the individual. Such data can be part of a computer record or manual record.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

2. Responsibilities

Overall responsibility for ensuring that the school meets the statutory requirements of any data protection legislation lies with the Governors and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Data Protection Officer (DPO).

The DPO is responsible for ensuring compliance with data protection legislation and this policy within the day-to-day activities of the school. The DPO is responsible for ensuring that appropriate training is provided for all staff.

All contractors who hold or collect personal data on behalf of the school by way of written contract are responsible for their own compliance with data protection legislation and must ensure that personal information is kept and processed in line with data protection legislation and only upon instruction from the school, via a contract.

3. The Requirements

Data protection legislation stipulates that anyone processing personal data must comply with principles of good practice; these principles are legally enforceable. The 6 principles require that personal data:

1. Shall be processed fairly and lawfully and transparently;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be kept secure ie protected by an appropriate degree of security.

In addition the data shall be processed in accordance with the rights of data subjects. (See Section 16 below)

Personal data shall also not be transferred to a country unless that country or territory ensures an adequate level of data protection or another secure method of transfer is guaranteed.

4. Notification

The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the school must be registered.

The school will review the Data Protection Register (https://ico.org.uk/esdwebpages/search) annually, prior to renewing its notification to the Information Commissioner.

5. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following at that initial point of collection:

- The identity of the data controller, eg the school;
- Contact details of the Data Protection Officer;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- What the lawful basis is for processing the data;
- Who the information will or may be shared with;
- If the data is transferred outside of the EU, and if yes, how is it kept secure;
- How long the data will be kept for; and
- How data subjects can exercise their rights.

The school will review its Privacy Notice annually and alert students and parents to any updates.

6. Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the GDPR has been satisfied.

Processing of special category (sensitive) personal data may only be carried out if a condition in Article 9 of the GDPR is met as well as one in Article 6.

7. Data Protection Officer

The school appoints a Data Protection Officer in line with the requirements of the GDPR.

8. Data Protection Impact Assessments

The school undertakes high risk Data Protection Impact Assessments in line with the requirements of the GDPR and as per the Information Commissioner's Office (ICO) guidance.

9. Data Breaches

All employees, governors, contractors, agents and representatives, volunteers and temporary staff shall report a security incident or data breach immediately to senior management and the school's Data Protection Officer.

The school reports any personal data breach to the ICO in line with the requirements of the GDPR.

10. Contracts

The school ensures that a legally binding contract is in place with all of its data processors in line with the requirements of the GDPR.

11. Consent

Where the school processes data with consent (for example, to publish photographs of children, to send direct marketing emails about school uniform for sale) it will ensure that the consent is freely given, specific, informed and unambiguous, and the consent is recorded.

12. Information Society Services

Where the school offers Information Society Services (online services with a commercial element) targeted at children, it will take reasonable steps to seek the consent of the child's parent if the child is under 13 years of age.

13. Direct Marketing

Where the school sends any direct marketing (the promotion of aims and ideals as well as selling goods and services) via electronic communications, eg email, SMS text, fax or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them, eg has ticked a box to 'opt in'.

15. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Other members of staff on a need to know basis;
- Relevant Parents;
- Other authorities if it is necessary in the public interest, eg prevention of crime, safeguarding;
- Other authorities, such as the Local Authority and schools to which a student may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Student Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

The school should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt, or statutory requirements conflict, legal advice should be obtained. Where there are safeguarding concerns, the matter should be referred to the school's Designated Safeguarding Lead (DSL).

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example, in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. Care must always be taken when there is any doubt about parental responsibility.

16. The Individual's Rights

Any person whose details are held by the school is entitled to ask for a copy of information held about them (or child for which they are responsible). They are entitled to see if the data held are accurate, and who it is shared with.

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month and in some instances, for education records, 15 school days. All staff must recognise and log such a request with the Data Protection Officer.

The school cannot charge for responding to a subject access request unless the request is repeated manifestly unfounded or excessive. The school can charge up to £50 (on a sliding scale for photocopying charges) for access to a pupil's Educational Record.

When providing the information the school must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Staff of the school must also recognise and log the following requests with the Data Protection Officer, and all must be answered within one month:

- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Portability
- Right to Object
- Right to Prevent Automated Processing
- Right to Complain

Further information about these rights can be found on the ICO website: https://ico.org.uk

17. Provision of Data to Children

In relation to the capacity of a child to make a subject access request, guidance provided by the ICO has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child is entitled to make the request on behalf of the child and receive a response.

Students who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

18. Parents' Rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the school is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child. The school has the right to ask the Child if they object to release of information to the Parent if the Child is deemed mature enough to make such a decision.

In addition, parents have their own independent right under The Education (Student Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records (as defined in the Education Act).

19. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are

visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. All removable devices, eg laptops, USB sticks, personal mobile phones and digital cameras should be password protected and/or encrypted wherever school data is being saved.

All members of staff should take care when transporting paper files between sites. No personal data is ever to be left unattended off site, eg in a car overnight, on view to family members when working at home.

All members of staff should take care when emailing personal data and always check the email address is correct and the right attachment has been attached. When copying to several people externally, all members of staff must always use the BC field and not the CC field nor create a group.

20. Maintenance of Up to Date Data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the school plus an additional period which the school has determined. The Data Protection Officer will ensure the school's retention procedures are in line with the GDPR.

21. Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. This must be answered within one month. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

22. Recording of Data

Records should be correct, unbiased, unambiguous, factual and clear. They should be kept in such a way that the individual concerned can understand them if they are requested. Records are also sometimes requested as part of legal processes and investigations. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the school's website will be required to give written consent unless it is a legal requirement (eg Governors' details). At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

23. Photographs

Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the school takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the school and, in particular, to record their wishes if they do not want photographs to be taken of their children.

24. Breach of the Policy

Non-compliance with the requirements of data protection legislation by the members of staff could lead to serious action being taken by third parties against the school. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the law, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

25. Further Information

Further advice and information about data protection legislation, including full details of exemptions, is available from the ICO website at www.ico.org.uk, or from Kirklees Council's Information Governance Team via information.governance@kirklees.gov.uk

26. Review of the Policy

This policy is to be reviewed annually.

27. Glossary

Data Controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Subject	The individual who the data or information is about
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the student or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner	The independent regulator who has responsibility to see that the data protection legislation is complied with. They can give advice on data protection issues and can enforce measures

	against individuals or organisations who do not comply with the law.
Notified Purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.
Personal Data	Defined as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' or an identifier (the school is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing. Just holding or storing the data constitutes processing.
Processed fairly and lawfully	Data must be processed in accordance with the provisions of data protection legislation. These include the data protection principles, the rights of the individual and notification.
Special Category (sensitive) Data	Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, or biometric or genetic data.
Subject Access Request	An individual's request for personal data under the General Data Protection Regulation.

Appendix one: Data Protection - Data Breach Procedure

Covering both Data Protection Act 1998 and GDPR which replaces the DP Act 1998 on 25 May 2018

Policy Statement
Holmfirth High 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 Holmfirth High 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 Holmfirth High 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".

- **Article 33 of the General Data Protection Regulations**
  Notification of a personal data breach to the supervisory authority

  1. *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

  2. *The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*

  3. *The notification referred to in paragraph 1 shall at least:*

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. *Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

5. *The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

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;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack, including 'phishing' or 'whaling';
- Hacking;
- 'Blagging' offences where information is obtained by deception;
- Unforeseen circumstances such as fire or flood.

Immediate Containment/Recovery

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Data Protection Officer (DPO) or, in their absence the Head Teacher. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The 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.

3. The DPO 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.

However, should the DPO require any expert guidance and assistance; they can contact the Information Governance Team at Kirklees Council. The Information Governance Team can be contacted either via telephone on 01484 221000 or by email **excluding any person identifiable data** to information.governance@kirklees.gov.uk.

4. The DPO 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. In such instances, advice from the school may wish to obtain advice from its legal support.

5. The DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    a. Attempting to recover lost equipment.

    b. 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 DPO.

    c. Contacting the Council's Marketing and Communications Department so that they can be prepared to handle any press enquiries. The Council's Press Office can be contacted by telephone on 01484 221000

    d. The use of back-ups to restore lost/damaged/stolen data.

    e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

    f. 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 DPO to fully investigate the breach. The DPO 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 (eg 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, such as harm to self, or finances, property or possessions.

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 due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office (ICO). A more detailed 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 initial investigation has taken place. The DPO should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the ICO must be notified within 72 hours of the breach under the GDPR. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able 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). 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

Review and Evaluation

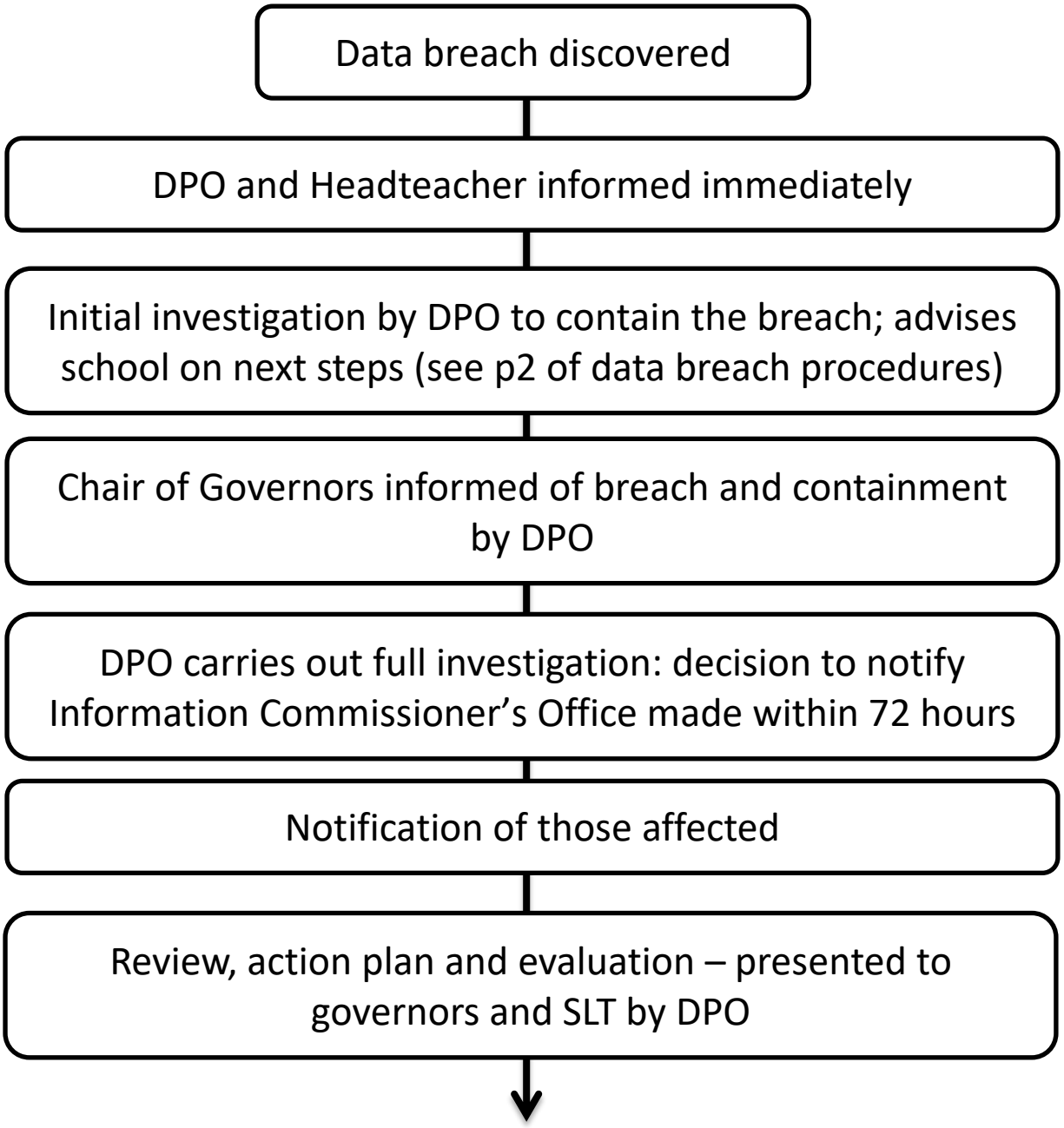
Once the initial aftermath of the breach is over, DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, 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 Human Resources or Internal Audit 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 DPO should ensure that staff are aware of the school's Data Protection policy and its requirements, including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Further Information
ICO website: https://ico.org.uk/for-organisations/report-a-breach/

FLOW CHART SHOWING ACTION TO BE TAKEN IN THE EVENT OF A DATA BREACH



Appendix two: The Individual's Rights

Any person whose details are held by the school is entitled to ask for a copy of information held about them (or child for which they are responsible). They are entitled to see if the data held are accurate, and who it is shared with.

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month and in some instances, for education records, 15 school days. All staff must recognise and log such a request with the Data Protection Officer.

The school cannot charge for responding to a subject access request unless the request is repeated manifestly unfounded or excessive. The school can charge up to £50 (on a sliding scale for photocopying charges) for access to a pupil's Educational Record.

When providing the information the school must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Staff of the school must also recognise and log the following requests with the Data Protection Officer, and all must be answered within one month:

- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Portability
- Right to Object
- Right to Prevent Automated Processing
- Right to Complain

Further information about these rights can be found on the ICO website: https://ico.org.uk