DURLSTON

Policy 2.20

Data Protection, Data Subject Rights for Staff and Data Breach Policy

Updated:	02.08.26
Owner:	BRS
Next Review date:	01.09.27

Durlston School 2.20 Data Protection, Data Subject Rights for Staff and Data Breach Policy

PART 1: DATA PROTECTION POLICY FOR STAFF

1 INTRODUCTION

1.1 Durlston School ('the school') is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information relating to the School and school community, including pupils, parents and staff.

1.2 This policy sets out how we comply with our data protection obligations set out in the UK General Data Protection Regulation (the "**UK GDPR**") and the Data Protection Act ("**DPA**") 2018, and seek to protect the personal data of our pupils, parents, staff, and other individuals who may come into contact with the School.

1.3 The aim of this policy is to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their duties.

1.4 The Head has appointed Barry Bates, the Bursar as the person with overall responsibility for data protection compliance, Data Compliance Lead ("**DCL"**). Any questions about this policy or requests for further information should be directed to them. The DCL may be contacted through the schools switchboard.

2 SCOPE

2.1 This policy applies to all staff. Any reference to the term staff in this policy includes employees, trustees, volunteers, consultants, contractors, interns, temporary workers, visiting music teachers (VMTs), any peripatetic workers and sports coaches, agency workers and casual workers.

2.2 Staff should refer to the School's privacy notices and, where appropriate, to other relevant policies, including those relating to information security, data retention, bring your own device (BYOD), and data breaches, which contain further information regarding the protection of personal data in those contexts.

2.3 We will review and update this policy on an annual basis in accordance with our data protection obligations. This policy does not form part of any employee's contract of employment or consultant's consultancy agreement, and we may amend, update or supplement it from time to time. We will circulate any new or materially modified policy to staff when it is adopted.

2.4 All staff are required to read and confirm that they understand this policy.

3 DEFINITIONS

3.1 This policy uses the following definitions:

Term	Meaning

Criminal offence data	means all personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings);
Data subject	means an individual to whom personal data relates;
Personal data	means any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other available information;
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 or special category data transmitted, stored or otherwise processed;
Processed / Processing	means any actions performed on personal data, including collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.
Special category personal data	means personal data afforded special protection by the UK GDPR. This includes, information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation;
Information Commissioner's Office (ICO)	means the UK's data protection and information regulator.

4 DATA PROTECTION PRINCIPLES

4.1 When processing personal data, the School and its staff must comply with the data protection principles set out in Article 5 of the UK GDPR as follows:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner ('***lawfulness, fairness and transparency***');

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes ('***purpose limitation***');

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes ('***data minimisation***');

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay ('***accuracy***');

4.1.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed ('***storage limitation***'); and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage ('***integrity and confidentiality***');

4.2 In addition, the School is also responsible for, and must be able to demonstrate compliance with the above principles ('***accountability***'). This means that the School will:

1.1.1. inform individuals about how and why we process their personal data, usually by way of a privacy notice;

1.1.2. be responsible for checking the quality and accuracy of the information;

1.1.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with our records retention policy;

1.1.4. ensure that when information is authorised for disposal it is disposed of / deleted appropriately;

1.1.5. ensure appropriate security measures to safeguard personal information whether it is held in paper files or electronically, and follow the requirements set out in our information security policy at all times;

1.1.6. share personal information with others only when it is necessary and legally appropriate to do so;

1.1.7. set out clear procedures for responding to requests for access to personal information known as subject access requests and other rights exercised by individuals in accordance with the UK GDPR (please see "Part 2: Data Subject Rights Policy" below); and

1.1.8. report any actual or suspected personal data breaches in accordance with the procedure set out in the Personal Data Breach Procedure.

5 LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 The School is responsible for ensuring that personal data is processed in a lawful, fair and transparent way. In relation to any processing activity we will, before the processing begins, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and identify which of the following legal bases for processing (as set out in Article 6 of the UK GDPR) is most appropriate:

(a) that the data subject has ***consented*** to the processing;

(b) that the processing is necessary for the ***performance of a contract*** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for ***compliance with a legal obligation*** to which the School is subject;

(d) that the processing is necessary for the ***protection of the vital interests*** of the data subject or another natural person;

(e) that the processing is necessary for the purposes of ***legitimate interests*** of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.4 where special category personal data or criminal offence data is processed, also identify a lawful condition (as set out in Articles 9 and 10 of the UK GDPR, and Schedule 1 of the DPA 2018) for processing this type of information, and document it.

5.2 When determining whether the legal basis of legitimate interests is appropriate, we will:

5.2.1 carry out a legitimate interests assessment ("**LIA**") (a type of light-touch risk assessment) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant risk to an individual's data protection rights, consider whether we also need to conduct a data protection impact assessment ("**DPIA**");

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

5.3 Where processing of personal data is likely to result in a high risk to individuals, we will, before commencing the processing, carry out a DPIA to assess:

5.3.1 whether the processing is necessary and proportionate in relation to its purpose;

5.3.2 the risks to individuals; and

5.3.3 what measures can be put in place to address those risks and protect personal information.

5.4 In order to comply with its transparency obligations, the School will issue privacy notices from time to time, informing data subjects about the personal data that we collect and hold, how they can expect personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6 PURPOSE LIMITATION

6.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with the purpose(s) identified.

6.2 You must not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and, where necessary, they have consented.

7 DATA MINIMISATION

7.1 The School will ensure that the processing of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

7.2 You may only collect personal data to the extent required for your duties, and should ensure that any personal data collected is adequate and relevant for the intended purposes. In order to do this, you should:

7.2.1 minimise the processing of personal data, for example, through redaction (i.e. obscuring or censoring text) and the deletion of long emails trails;

7.2.2 anonymise personal data where appropriate;

7.2.3 pseudonymise personal data where possible, for example, through the use of initials rather than full names; and

7.2.4 ensure that when personal data is no longer needed, it is deleted in accordance with the Records Retention and Deletion Policy.

8 ACCURACY

8.1 Personal data must be accurate and kept up to date. It must be corrected or deleted without delay when it is inaccurate.

8.2 Staff have a responsibility for helping the School keep their own personal data up to date. You should complete a self-declaration on a low-level concerns form (See Policy) if the information you have provided to the School and its schools changes, for example if you move house or change details of the bank or building society account to which you are paid. This helps the School comply with its wider data protection obligations and can reduce the likelihood of a data breach occurring. The School also asks parents to inform them of any changes to their or their child's personal data.

9 STORAGE LIMITATION

9.1 Personal data should not be kept for any longer than is necessary for the purposes for which the personal data is processed.

9.2 The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow guidance contained in the Records Retention and Deletion Policy, which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

9.3 Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

10 INTEGRITY AND CONFIDENTIALITY

10.1 The School will use appropriate technical and organisational measures in accordance with our information security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10.2 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DCL.

10.3 All staff have an obligation to report actual or suspected personal data breaches. Please refer to the Personal Data Breach Procedure for further guidance on reporting procedures and obligations.

11 DOCUMENTATION AND RECORDS

11.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category data or criminal offence data, including:

11.1.1 the purposes of the processing;

11.1.2 a description of the categories of individuals and categories of personal data;

11.1.3 categories of recipients of personal data;

11.1.4 where relevant, details of transfers of personal data outside the UK, including documentation of the transfer mechanism safeguards in place;

11.1.5 where possible, retention schedules; and

11.1.6 where possible, a description of technical and organisational security measures.

11.2 As part of our record of processing activities we document, or link to documentation, on:

11.2.1 information required for privacy notices;

11.2.2 records of consent;

11.2.3 controller-processor contracts;

11.2.4 the location of personal information;

11.2.5 DPIAs; and

11.2.6 records of personal data breaches.

11.3 If we process special category data or criminal offence data, we will keep written records of:

11.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

11.3.2 the lawful basis and additional conditions relied upon to process this information; and

11.3.3 whether we retain and erase the personal information in accordance with our Records Retention and Deletion Policy and, if not, the reasons for not following the Records Retention and Deletion Policy.

11.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly.

12 INDIVIDUAL OBLIGATIONS

12.1 You may have access to the personal information of others including members of staff, parents, pupils, and other third parties who may come into contact with the School in the course of your employment or engagement. If so, the School expects you to help meet its data protection obligations to those individuals.

12.2 If you have access to personal data, you must:

12.2.1 only access the personal data that you have authority to access, and only for authorised purposes;

12.2.2 only allow other staff to access personal data if they have appropriate authorisation;

12.2.3 only allow individuals who are not staff to access personal data if you have specific authority to do so from the DCL or school DCL;

12.2.4 keep personal data secure (e.g. by complying with the obligations set out in the Information Security Policy) ; and

12.2.5 to the extent that you may use personal devices for work purposes, comply with the School's BYOD Policy.

13 INTERNATIONAL TRANSFERS

The School may transfer personal data outside the UK on the basis that that country, territory or organisation is designated as having an adequate level of protection, or that the organisation receiving the information has provided adequate safeguards to ensure the protection of personal data.

14 TRAINING

The School will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for

implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

15 WORKING REMOTELY

15.1 As part of our commitment to flexible working, the School supports homeworking in appropriate circumstances, either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular basis (full or part-time).

15.2 Working remotely can lead to increased risk in terms of the security of School information (including personal data) and communications systems. When working remotely, you must comply with all relevant policies, including our:

15.2.1 Staff Data Protection Policy (this policy);

15.2.2 Information Security Policy;

15.2.3 Bring Your Own Device (BYOD) policy;

15.2.4 Records Retention and Deletion Policy; and

at all times and to attend any additional training on data protection and confidentiality as may be required by the School.

16 CONSEQUENCES OF FAILING TO COMPLY

16.1 The School takes compliance with this policy very seriously. Failure to comply with the policy:

16.1.1 puts at risk the individuals whose personal information is being processed; and

16.1.2 carries the risk of significant sanctions for the individual and the School; and

16.1.3 may, in some circumstances, amount to a criminal offence by the individual.

16.2 Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of your relationship with the School.

17 CONTACT

If anyone has any concerns or questions in relation to this policy they should contact the DCL using the contact details detailed at the start of this policy.

PART 2: DATA SUBJECT RIGHTS POLICY

18 DATA SUBJECT RIGHTS AND REQUESTS

18.1 Data subjects have rights in relation to their personal data. This includes the right to:

18.1.1 to be ***informed*** about how, why and on what basis that information is processed (the School usually provides this information to data subjects via its Privacy Notice(s));

18.1.2 to obtain confirmation that information is being processed and to obtain ***access*** to it and certain other information by making a subject access request;

18.1.3 to have personal data ***corrected*** if it is inaccurate or incomplete (known as *the right of rectification*);

18.1.4 to have personal data ***erased*** in certain circumstances (sometimes known as *the right to be forgotten*);

18.1.5 to ***restrict the processing*** of personal their personal data in certain circumstances (e.g. if there is a complaint about accuracy);

18.1.6 to ***object*** to the processing of their personal data in certain circumstances;

18.1.7 to ***receive*** personal data that they have provided in a structured, commonly used and machine-readable format and to request that their personal data is ***transferred*** to another organisation (known as *the right to data portability*)

19 SUBJECT ACCESS REQUESTS

19.1 Anybody has the right to ask the School for a copy of any personal information held about them, together with other information about how their information is used (known as supplementary information (see section 19.2 below). This legal right is called the right of access, often referred to as a subject access request or SAR.

19.1.1 There are some legal exemptions that mean that requesters may not always be entitled to a copy of all of their personal information that we hold.

19.2 As part of a subject access request, data subjects are entitled to the following supplementary information:

19.2.1 whether their personal data is being processed by the School;

19.2.2 the purposes of the processing;

19.2.3 the categories of personal data concerned;

19.2.4 the recipients or categories of recipient to whom their personal data have been or will be disclosed;

19.2.5 the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;

19.2.6 the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;

19.2.7 their right to lodge a complaint with the ICO;

19.2.8 where the personal data are not collected from the individual, any available information as to their source; and

19.2.9 details of the safeguards in place for any transfers of their data to locations outside the UK.

19.3 If you, as a member of staff, receive a SAR from a pupil, parent or carer or other person, you should immediately forward it to the School DCL (SDCL) or School DCL as appropriate. The School has a legal

duty to deal with SARs without delay and at the latest within one month of receipt (subject to the rights of the School to extend the time limit for response by a further two months, considering the complexity and number of the requests, in accordance with Article 12(3) of the UK GDPR). The SDCL should ensure that the Head and DCL are updated on any SARs received.

19.4 Any individual, including a child or young person, may appoint another person to request access to their records. In such circumstances the School must have written evidence that the individual has authorised the person to make the request and the DCL or SDCL must be confident of the identity of the individual making the request.

19.5 Where a child or young person lacks capacity to understand their rights and the implications of making a subject access request (e.g. due to their age or some other reason) a third party, such as a parent or carer, can make a request on their behalf. The DCL or SDCL must, however, be satisfied that:

19.5.1 the child or young person lacks sufficient understanding of their own data rights; *and*

19.5.2 the request made on behalf of the child or young person is made in the child or young person's best interests.

19.6 Access to personal data may be restricted or refused in instances where an exemption under the DPA 2018 applies. For example, the relevant information is covered by legal advice privilege or information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The School must decide whether to apply any potential exemption (taking legal advice where appropriate), based on the circumstances of a particular request.

19.7 A subject access request may be made verbally or in writing. Where possible, the School prefers requests to be made in writing. The School may ask the data subject for any further information reasonably required to locate the information.

19.8 All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by the DCL or SDCL. Any disclosure can only take place after the response is approved by the DCL. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the supplementary information the requestor is entitled to (please see section 2.2).

19.9 Where some of the data in a document cannot be disclosed a copy of the full document and the altered document should be retained, with the reason why the document was altered.

20 RIGHT TO RECTIFICATION

20.1 Data subjects have the right to request the rectification of inaccurate or incomplete data verbally or in writing. Any request for rectification should be sent to the SDCL or DCL immediately.

20.2 Where personal data is identified as inaccurate or incomplete, it shall be amended and the data subject notified of the same without undue delay and in any event within one month (unless this deadline is extended in accordance with the UK GDPR).

20.3 Where a request is refused, the request and reasons for refusal shall be documented and notice of refusal should be provided to the individual within a month of receipt of the request. The School will

include in its response the reasons why the request has been refused and information about the individual's right to complain to the ICO and to bring a civil claim.

21 RIGHT TO ERASURE

21.1 Individuals have a right, in certain circumstances, to have their personal data permanently erased. Individuals may exercise this right in writing or verbally.

21.2 The right to erasure is also known as the 'right to be forgotten' and arises in the following circumstances:

21.2.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

21.2.2 where consent is the legal basis for processing and that consent is withdrawn;

21.2.3 where legitimate interests is the legal basis for processing and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue processing;

21.2.4 where the School is processing the personal data for direct marketing purposes and the individual objects to that processing;

21.2.5 where personal data is being unlawfully processed;

21.2.6 where there is a legal obligation on the School to delete the personal data; or

21.2.7 where the School has processed personal data based upon consent given by a child, particular weight should be given to any request for erasure. Further details about the right to erasure and children's personal data can be read in the ICO guidance on children's privacy.

21.3 Any request for erasure should be sent to the SDCL or DCL immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

21.4 The DCL will determine the outcome of any request for erasure of personal data. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, the School will inform those organisations of the request unless this proves impossible or involves disproportionate effort.

21.5 Where a request is refused, the School will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

22 RIGHT TO RESTRICT PROCESSING

22.1 In the following circumstances, individuals have the right to request the restriction or suppression of their personal data in writing or verbally:

22.1.1 where the accuracy of personal data has been contested, during the period when the School is attempting to verify the accuracy of the data;

22.1.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

22.1.3 where personal data would normally be deleted, but the individual has requested that their personal data be kept for the purpose of the establishment, exercise or defence of a legal claim;

22.1.4 where there has been an objection to the processing, pending the outcome of any decision.

22.2 Any request for restriction should be sent to the SDCL or DCL immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

22.3 The DCL will determine the outcome of any request for restriction of processing personal data. As matter of good practice, the School will automatically restrict the processing whilst considering the accuracy or legitimate grounds for processing the personal data in question.

22.4 Where processing has been restricted, such personal data shall (with the exception of storage) be processed only in the following circumstances:

22.4.1 with the consent of the data subject;

22.4.2 where processing is necessary for the establishment, exercise or defence of legal claims;

22.4.3 for the protection of rights of another person (including a company); or

22.4.4 for reasons of important public interest.

22.5 If the School has disclosed the personal data in question to others, it will contact each recipient to inform them of the restriction, unless this proves impossible or involves disproportionate effort.

22.6 Once the School has determined the accuracy of the data, or whether the School's legitimate grounds override those of the data subject, the School may decide to lift the restriction. The School will inform the requestor before the restriction is lifted.

22.7 Where a request is refused, the School will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

23 RIGHT TO OBJECT

23.1 Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purposes. This right is absolute and where such an objection is made the School will stop processing personal data for this purpose.

23.2 An individual also has the right to object to the processing of their personal data on the legal basis of:

23.2.1 a task carried out in the public interest;

23.2.2 the exercise of official authority vested in the School; or

23.2.3 the legitimate interests of the School or a third party.

23.3 Where such an objection is made, it must be sent to the SDCL or DCL immediately. The SDCL or DCL will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the information is required for the establishment, exercise or defence of legal proceedings.

23.4 The SDCL or DCL is responsible for notifying the individual of the outcome of their assessment without undue delay and within one calendar month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR). If the request is refused, the response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

24 RIGHT TO DATA PORTABILITY

24.1 Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to require the School to transmit that personal data directly to another data controller in certain circumstances (where feasible).

24.2 If such a request for this is made, it should be forwarded to the SDCL or DCL immediately and this will be reviewed and actioned as necessary.

PART 3: DATA BREACH POLICY

25. Policy Statement

25.1 Durlston 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 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 procedure applies to all personal and sensitive data held by Durlston) and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

26. Purpose

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

27. Legal Context

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

a) 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.

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

c) The notification referred to in paragraph 1 shall at least:

- 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;

- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- 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.

d) 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.

e) 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.

28. Types of Breach

28.1 Data protection breaches could be caused by a number of factors. A number of examples are shown below:-

- 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;
- Hacking.

29. Managing a Data Breach

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

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

2. The Head Teacher/DPO (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 Systems Manager.

3. The Head Teacher/DPO (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 Head Teacher/DPO (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. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) 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 local authority's Data Protection Officer, 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 Head Teacher/DPO (or nominated representative).

c) Contacting the local authority's Public Relations Team, so that they can be prepared to handle any press enquiries.

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.

30. Investigation

30.1 In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (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 were 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

30.2 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. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

31. Notification

31.1 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 Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach.
Every incident should be considered on a case by case basis.

31.2 When notifying individuals, specific and clear advice will be given on what they can do to protect themselves

and what the School is able to do to help them. They will also be advised of the opportunity to make a formal complaint if they wish (in accordance with the School's Complaints Procedure). The notification to individuals should include a description of how and when the breach occurred, what data was involved and details of what action has been taken to mitigate the risks posed by the breach.

32. Review and Evaluation

32.1 Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) 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 Management Team and Full Governors' meeting for discussion. If systemic or ongoing problems are identified, then an action plan will 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.

33. Implementation

33.1 The Head Teacher/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.

34. Policy Review

34.1 This policy will be reviewed annually or sooner should there be legislative changes, new case law or guidance, or following the investigation of a breach which identified a need for procedural changes.