Data Protection Policy
(including Privacy Notices for Pupils & Workforce)

Date of last review: **5 February 2020**

Date of next review: **February 2021**

Reviewed & Approved by: **Governing Body**

Scope of the Policy

This policy is intended to ensure that personal information held by Whitecross Nursery School is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing, disclosure and destruction of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Pupils, parents and staff have the right to access information held by the school. The most important rights are contained in the following legislation:

- Data Protection Act 2018
- Education (Pupil Information) (England) Regulations 2005
- Freedom of Information Act 2000

What is the General Data Protection Regulation (GDPR)?

This is a European Directive that will be brought into UK law with an updated Data Protection Act for May 2018. Brexit will not change it.

The Data Protection Act 1998, repealed and replaced with the Data Protection Act 2018.

What is the point of the GDPR?

The GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identified them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school also has to publish a Privacy / Fair Processing Notice on the website.

What are the key principles of the GDPR?

Lawfulness, transparency and fairness

School must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the website. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects Rights'.

Collect data for a specific purpose and use it for that purpose

So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention

The School retains records for the length of time required by law.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Electronic devices are password protected and paper files are kept in locked cupboards.

Who is a 'data subject'?

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for or are a parent of at school. This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.
When we receive a request we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information in this DPA policy.

Who is a 'data controller'?

We have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

Our school governing body is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school

- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & Non Compliance

If there is non compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

See Appendix 4

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.
However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

CCTV Policy

Please also see the CCTV and IT Security policy

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:- Detection and prevention of crime
School staff disciplinary procedures
Pupil behaviour and exclusion management processes
To assist the school in complying with legal and regulatory obligations

Data Protection Officer

We have a Data Protection Officer whose role is to:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Our DPO is John Walker whose contact details are J A Walker Solicitor e-mail john@jawalker.co.uk

Physical Security

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Headteacher is responsible for authorising access to secure areas along with Senior Teacher and School Business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDRP and DPA compliance.

Hardware is disposed / recycled by IT Technician.
Hard copy files are destroyed by staff
Servers and Hard drives are cleansed by IT Technician.
Portable and removable storage are destroyed / cleaned/ recycled by IT Technician.

Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review
A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

APPENDIX 1

Procedures for Requesting Information from the School

Requests for information under the Data Protection Act are called Subject Access Requests.

To access personal data the request must be made in writing, which includes email, and be addressed to the Head Teacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

A non-refundable fee of £10 will be charged in advance; the school will acknowledge receipt of the request as soon as possible after receipt of the payment of the fee. The response time for subject access requests, once officially received, is 40 calendar days. However, the 40 days will not commence until after receipt of fees or clarification of information sought. Any delay will be explained in writing to the person making the request.

Maintained schools:

A request to access a pupil's educational record should be made in writing to the Board of Governors. This covers information that comes from a teacher or other employee of a local authority or school, the pupil or parent, and is processed by or for the school's governing body or teacher, except for information the teacher has solely for their own use. A request for an educational record must receive a response within 15 school days.

1. Process

1.1 The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

1.2 Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

1.3 The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

1.4 Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

1.5 Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

1.6 If there are concerns over the disclosure of information then additional advice should be sought.

1.7 Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

1.7 Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

2. Feedback and Complaints

If you require further assistance or wish to make a complaint regarding information you have received or been refused then initially this should be addressed to the Chair of Governors, Whitecross Nursery School, Watson Street, Derby DE1 3PJ.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Data Protection Act 1998 and that deals with formal complaints. They can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Enquiry/Information Line: 01625 545 700
Website: www.informationcommissioner.gov.uk

Appendix 2

Privacy Notice – Pupil Data

Introduction

As a school we collect a significant amount of information about our pupils. This notice explains why we collect the information, how we use it, the type of information we collect and our lawful reasons to do so.

Why do we collect data?

We collect and use pupil data to:-

- Fulfil our statutory obligations to safeguard and protect children and vulnerable people
- Enable targeted, personalised learning for pupils
- Manage behaviour and effective discipline
- Monitor our effectiveness
- Comply with our legal obligations to share data
- Support pupils to fulfil their potential
- Keep pupils, parents and carers informed about school events and school news

Our Legal Obligations

We must make sure that information we collect and use about pupils is in line with the GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data, and that if we share that with another organisation or individual we must have a legal basis to do so.
The lawful basis for schools to collect information comes from a variety of sources, such as the Education Act 1996, Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013, Article 6 and Article 9 of the GDPR.
The Department for Education and Local Authorities require us to collect certain information and report back to them. This is called a 'public task' and is recognised in law as it is necessary to provide the information.
We also have obligations to collect data about children who are at risk of suffering harm, and to share that with other agencies who have a responsibility to safeguard children, such as the police and social care.
We also share information about pupils who may need or have an Education Health and Care Plan (or Statement of Special Educational Needs). Medical teams have access to some information about pupils, either by agreement or because the law says we must share that information, for example school nurses may visit the school.
Counselling services, careers services, occupational therapists are the type of people we will share information with, so long as we have consent or are required by law to do so.
We must keep up to date information about parents and carers for emergency contacts.

How we use the data

In school we also use various third party tools to make sure that pupils' best interests are advanced. We also record details about progress, attainment and pupil development to support future planning and learning.
We use software to track progress and attainment.
We use data to manage and monitor pastoral needs and attendance/absences so that suitable strategies can be planned if required.
This includes financial software to manage school budgets, which may include some pupil data.
Data can be used to monitor school effectiveness, the impact of intervention and learning styles across groups of pupils as well as individual children.

We may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the School properly. We might need to share pupil information with them if this is relevant to their work.

We also use contact information to keep pupils, parents, carers up to date about school events.

What type of data is collected?

The DfE and government requires us to collect a lot of data by law, so that they can monitor and support schools more widely, as well as checking on individual schools effectiveness.

The categories of pupil information that the school collects, holds and shares include the following:

- Personal information – e.g. names, pupil numbers and addresses
- Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility
- Attendance information – e.g. number of absences and absence reasons
- Assessment information – e.g. national curriculum assessment results
- Relevant medical information and social care
- Information relating to SEND and health needs
- Behavioural information – e.g. number of temporary exclusions

CCTV, photos and video recordings of you are also personal information.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process

and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Sue Silcock on 01332 371876 or call in at the school office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact Sue Silcock on 01332 371876 or call in at the school office.

More information about Data Protection and Our Policies

How we manage the data and our responsibilities to look after and share data is explained in our Data protection Policy, and connected policies, which are also available on our website.
If you feel that data about your child is not accurate, or no longer needed please contact the schools office. Our complaints policy explains what to do if there is a dispute. Subject Access Requests are dealt with by the specific policy on the website.

Appendix 3

Privacy Notice School Workforce

This privacy notice explains how we collect, process and manage information for the school workforce. That includes employed members of staff, volunteers, including trustees and governors, trainee teachers, apprentices and work experience/workplace placements.

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- medical information
- other personal information
- references

We use and share information to comply with statutory, regulatory, practice and contractual obligations. These may include, but are not limited to:-

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- pay salaries and pension contributions
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- comply with guidance such as 'Working Together' and safeguarding obligations
- facilitating good governance
- internal reviews and quality monitoring
- CPD and staffing issues

If we are required to comply with other legal obligations not listed above we will share data only when it is lawful to do so.

The lawful basis on which we collect and process this information

We must make sure that information we collect and use about pupils is in line with the GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data, and that if we share that with another organisation or individual we must have a legal basis to do so. The lawful basis for schools to collecting and processing information comes from a variety of sources, such as the Article 6 and Article 9 of the GDPR, the Safeguarding of Vulnerable Groups Act 2006. We also have obligations to organisations such as HMRC and the Department of Work and Pensions.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on

a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for in accordance with our HR and Retention Policy

Who we share this information with

We may share this information with organisations such as:

- our local authority
- the Department for Education (DfE)
- Safeguarding and protection for children and vulnerable adults
- Payroll services
- Legal Advisers
- Insurance providers
- HMRC
- Teacher Pension Scheme and the Local Government Pension Scheme (and other pension providers
- Health professionals

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.
We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-

collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the School Business Manager on 01332 371876 or call in at the school office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

More details about how we use and manage data can be found in the 'Data Processing Notices – Common Principles and Processes', the Data protection Policy and other relevant polices for the School Workforce on the website.

Appendix 4

Data Protection Breach & Non Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / GDPR breach. The 'Data Breach Flowchart' outlines the process.
The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported. Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

The breach notification form will be completed and the breach register updated.
If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

The breach report will be within 72 hours of becoming aware of the breach.
It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	School Officer