



Data Protection Policy & Procedures

Date of last review: Summer 2019

Introduction

Our school gathers and uses personal information about staff, pupils, parents and other individuals who come into contact with the school to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Duty on Schools

Schools 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. Schools also have a duty to issue a Privacy Notice (see appendix 1) to all pupils/parents, which summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy and set of procedures are intended to ensure that personal information 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, on tape or disk, or otherwise electronically.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This includes, but is not limited to, their name, address, date of birth, photograph and bank details.

What is Sensitive Personal Information?

Sensitive personal data includes: an individual's racial or ethnic origin; religious or political beliefs; trade union membership; physical or mental health; sex life or orientation; criminal offences and court proceedings. Our Appropriate Policy Document gives a more detailed explanation of how we lawfully process special categories of personal data.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up-to-date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
7. Personal data shall be kept secure ie protected by an appropriate degree of security.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Our Commitment

Our school is committed to maintaining the above principles at all times. Therefore we will:

- Register as Data Controllers with the Information Commissioner's Office (ICO) detailing the information held and its use;
- Inform individuals why the information is being collected and when it is collected;
- Inform individuals when their information is shared and why and with whom it was shared;
- Obtain consent before processing Sensitive Personal Data, even if consent is implied within a relevant privacy notice, unless one of the other conditions for processing in the Data Protection Act applies;
- Check the quality and the accuracy of the information we hold;
- Ensure that only authorised personnel have access to data;
- Ensure that robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure;
- Ensure that information is not retained for longer than is necessary and that when data is destroyed it is done so appropriately and securely;
- Comply with the duty to respond to requests for access to personal information, known as subject access requests;
- Issue a Privacy Notice which summarises the information held by us;
- Ensure our staff and governors are aware of and understand our policies and procedures.

Legal Basis for Processing Data

The legal basis by which we will process data include:

- **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- **Contract** - 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;
- **Legal** - processing is necessary for compliance with a legal obligation to which the controller is subject;
- **Vital interests** - processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- **Public task** - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- **Legitimate interests** - processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Retention of Information

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule. The schedule lists types of records used by the school, the rationale for keeping this information and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements. Paper and electronic records will be regularly monitored by the School Business Manager. Paper documents that are retained for a lengthy period are likely to be converted to digital format.

Deletion of Information

Where records have been identified for destruction they will be disposed of in an appropriate way. All information will be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances. All paper records containing personal information, or sensitive policy information will be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant.

All electronic information will be deleted. The School maintains a database of records which have been destroyed together with who authorised their destruction. When destroying documents, the appropriate staff member should record: the file reference (or other unique identifier); the file title/description; the number of files; and the name of the authorising officer.

Guidance for Home Working

Where data is needed when working away from the school site, additional safeguards must be employed. Only data required to complete the work should be taken and staff are issued with encrypted USB sticks for the purpose of keeping this data secure. Additional guidance is set out in Appendix D.

Rights of access to information – Subject Access Requests (SAR)

Pupils, parents and guardians have two distinct rights of access to information held by schools about pupils as set out below. In addition, the school may hold some information about parents and guardians and the right of access to this is covered by number one below only:

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

Requests for small amounts of data that are readily available, such as a test result, are unlikely to require a SAR. Appendix B details the process for responding to a Subject Access Request.

Dealing with a Data Breach

Data protection breaches could be caused by a number of factors, such as: 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 or hacking.

Whilst we make every attempt to keep data secure, it is recognised that data may be breached or lost. We have put measures in place to limit the risk of data breach / loss. Regular updates and training are provided to update / remind staff. Appendix F sets out the process for dealing with a data breach.

Contacts

If you have any enquires in relation to this policy and procedures, please contact the headteacher who will also act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453.

Complaints

Complaints will be dealt with in accordance with the School's Complaints Policy, a copy of which is available from the school office. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator) via www.ico.gov.uk or telephone 01625 5457453.

Monitoring and Dissemination

This policy will be reviewed as required. The policy review will be undertaken by the Headteacher, or nominated representative, before being approved and adopted by the Governing Body. The School commits to publishing the latest ratified Data Protection Policy on the School's website and hard copies are available on request from the School Office.

Appendices:

Appendix A	Privacy Notices for Pupils, Parents & Employees
Appendix B	Procedures for responding to Subject Access Requests (SAR)
Appendix C	Retention of Data Schedule
Appendix D	Data Protection Guidance for Teachers
Appendix E	Guidance for Home Working
Appendix F	Dealing with a data breach

Appendix A: Privacy Notice for Pupils & Parents

Wendover CE Junior School collects data and information about our pupils and parents / carers so that we can run effectively as a school. We are a primary, local authority maintained school and the data controller for the data we process on pupils attending our school. This privacy notice explains how and why we collect pupil and parent / carer data, what we do with it and what rights parents and pupils have.

If you would like to discuss anything in this privacy notice, please contact our Administration Manager at admin@wendoverjunior.co.uk or our Data Protection Officer at nicola@schoolsdp.com.

Information we hold

We currently collect and process the following information:

- a. personal identifiers and contacts (such as name, unique pupil number, contact details and address);
- b. characteristics (such as ethnicity, language, pupil premium and free school meal eligibility);
- c. safeguarding information (such as court orders and professional involvement);
- d. special educational needs (including the needs and ranking);
- e. medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements);
- f. attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended);
- g. assessment and attainment (such as key stage 1 and phonics results);
- h. behavioural information (such as exclusions and any relevant alternative provision put in place).

How we collect the information and why we have it

We collect information about pupils and parents / carers before they join the school and update it during their time on the roll as and when new information is acquired. It is used to:

- a. to support pupil learning and progress;
- b. to run the school safely and effectively and protect the welfare of everyone in school;
- c. to meet our legal obligations, such as data sharing.

Most of the personal information we process is provided to us directly by you but we also receive personal information when pupils join the school from:

- a. other schools and nursery settings;
- b. from the local authority.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for this processing are:

- a. your consent. You are able to remove your consent at any time. You can do this by contacting
- b. we have a contractual obligation;
- c. we have a legal obligation;
- d. we need it to perform a public task;
- e. we have a vital interest;
- f. we have a legitimate interest.

Some personal information requires extra protection as it is considered more sensitive. This includes race, ethnicity, religious beliefs, medical conditions, genetic information and biometric data, criminal convictions.

If we are processing special category data, our lawful bases will also include one of the following:

- a. we have explicit consent;
- b. to meet our obligations as a controller or those of data subjects;
- c. to meet our public interest task of keeping pupils safe.

What we do with the information

We use the information you have given us to:

- support pupil learning
- monitor and report on pupil progress
- provide appropriate pastoral care
- assess the quality of our services

- comply with the law regarding data sharing
- protect the welfare of pupils and others in the school
- run the school safely and effectively
- promote the school, including taking photographic images
- communicate with parents / carers.

We may share this information with:

- schools that pupils attend after leaving us
- our local authority, Buckinghamshire County Council
- the Department for Education (DfE) (statutory data collections)
- school governors / trustees
- companies providing services to the school, e.g. catering, photography, communication services.

From time to time, we may also share pupil information with other third parties including the following:

- the Police and law enforcement agencies
- NHS health professionals including the school nurse
- Educational psychologists
- Education Welfare Officers
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools.

In the event that we share personal data about pupils with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

How we store your information

A significant amount of personal data is stored electronically, for example, on our MIS (management information system) database and curriculum network. Some information may also be stored in hard copy format in lockable filing cabinets.

We hold pupil and parent / carers' data in line with our retention schedule which is available from the school office.

Your data protection rights

Under data protection law parents / carers and pupils have the right to request access to information about them that we hold (a subject access request).

To make a request for your personal information or to be given access to your child's educational record, please contact the school office or our data protection officer (see contact details at the start of this privacy notice). Where a child does not have the maturity to make their own requests for personal data, parents may do so on their behalf in a primary school setting.

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
- a right to seek redress either through the ICO or through the courts.

Under GDPR you are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Parents of pupils who attend a maintained school have a separate statutory right to access their child's educational record. Upon receipt of a written request for a pupil's educational record, the school will respond to it within 15 school days. This is an independent legal right of parents which falls outside of the GDPR.

How you can help us

As the school has limited staff resources outside of term time, we encourage parents to submit requests for information during term time and to avoid sending a request during periods when the school is closed, or is about to close for the holidays, where possible. This will assist us in responding to your request as promptly as possible.

For further information about how we handle subject access requests, please see our Data Protection Policy.

Any concerns

If you have a concern about the way we are collecting or using your or your child's personal data, you should raise your concern with us in the first instance. You can also complain to the Information Commissioner's Office (ICO) if you are unhappy with how we have used your data:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Telephone: 0303 123 1113.

If you require more information about how the Local Authority and/or Department of Education store and use your information, then please go to the following websites:

LA: www.buckscc.gov.uk/privacynotice

DfE: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Privacy Notice for Employees: How we use workforce information

We, **Wendover CE Junior School**, process personal data relating to those we employ, or otherwise engage to work at our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid.

The categories of school information that we process include:

- personal information (such as name, address, DOB, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- medical information (such as conditions which require adjustments to the workplace)
- qualifications

Why we collect and use workforce information

We use workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

Under the General Data Protection Regulation (GDPR), the legal basis we rely on for processing personal information for general purposes are:

- Article 6.1.e states that the use of personal data is justified if 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. In this instance, the requirement for the school to deliver education under the Education Act (1996) requires us to collect information to deliver this service.
- Article 9 covers the use of sensitive personal information (this includes health and social care information). This is justified either by article 9.2.a (consent from the data subject) or article 9.2.e (processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services).

Collecting workforce information

We collect personal information via application forms, data collection sheets and contracts. Workforce data is essential for the school's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely in accordance with our data retention policy.

Who we share workforce information with

We routinely share this information with:

- Bucks County Council
- the Department for Education (DfE)

Why we share school workforce information

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

Local authority (Bucks County Council)

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

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the DfE for the purpose of those data collections, under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#). For more information, please see 'How Government uses your data' section.

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 headteacher or business manager.

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
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact 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 the headteacher or business manager.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

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>.

Sharing by the Department

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.

To contact the department: <https://www.gov.uk/contact-dfe>

Appendix B: Procedure for responding to Subject Access Requests (SAR)

1. Requests for information must be made in writing, including email, and be addressed to the headteacher. It should clearly identify the information required.
2. The identity of the requestor must be established before the disclosure of any information. When requesting data on a pupil, checks will also be carried out regarding proof of relationship to the child. Two forms of identity will need to be submitted in person:
 - passport
 - driving licence
 - utility bills (less than 3 months old)
 - birth/marriage certificate
 - P45/P60
 - credit card or mortgage statement (less than 3 months old)
3. Any individual has the right of access to information held about them. The school will consult with the parent in the event that a request is made by a child.
4. The school may charge for the provision of information if it is considered to be excessive, repetitive or requires additional copies. The fee will be based on the administrative cost of providing the information. Additionally, the school will comply to the request within 90 days (the requester will be informed of this on receipt of the request).
5. The response time for a subject access requests, once officially received, is 15 school days where educational records are sought and 30 calendar days otherwise from receipt.
6. The Data Protection Act 1998 allows exemptions as to the provision of some information therefore all information will be reviewed prior to disclosure.
7. Third party information is that which has been provided by or identifies another person. Before disclosing third party information, consent will be obtained. Otherwise this information will be redacted.
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed (this includes information relating to a child at risk of abuse or information relating to court proceedings).
9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained.
10. Advice will be sought if there are concerns over the disclosure of information.
11. Information can be provided for viewing at the school, or a face to face handover of the response to the requester. All posted responses will be by registered/recorded mail.

Contacts

If you have any enquires in relation to this policy and procedures, please contact the headteacher who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453.

Appendix C: Retention of Data Schedule

File Description	Reason for Retention	Retention Period
Employment Records		
Job applications and interview records of unsuccessful candidates	Records held until successful candidate(s) have accepted offers and appointment processed	Maximum one month after notifying unsuccessful candidates
Job applications and interview records of successful candidates	Personnel file	Retained while employed; destroyed within one month of leaving employment
Written particulars of employment, contracts of employment, changes to terms and conditions	Personnel file	Retained while employed; destroyed within one year of leaving employment
DBS checks and disclosures of criminal records form	Confirmation of check result – SCR requirement	Retained whilst employed; destroyed within one month of leaving employment
Change of personal details notifications	Personnel file	Retained while employed; destroyed within one month of leaving employment
Emergency contact details	Personnel file	Retained while employed; destroyed within one month of leaving employment
Personnel and training records	Personnel file	Retained while employed; destroyed within one month of leaving employment
Annual leave records	Personnel file	Retained while employed; destroyed within one month of leaving employment
Disciplinary records	Personnel file	6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is upheld	Confidential file (held by HT)	10 years from date of allegation or the person's normal retirement age Malicious allegations will be destroyed when employment ceases
Maternity/adoption/paternity leave records	Personnel file	Retained while employed; destroyed within one month of leaving employment
Payroll and salary records	Audit requirement	6 years after the tax year they relate to
Records relating to casual and supply staff	Audit requirement	6 years from the tax year they relate to
General Records		
School development plans	Progress Tracking	3 years from the life of the plan
Visitor signing in sheets	Safeguarding	1 year
Newsletters and general correspondence	School development	1 year
Health & Safety Records		
H&S consultations	HSE requirement	Permanently
H&S risk assessments	HSE requirement	3 years from life of RA
Any reportable accident, injury or death in connection with work	HSE requirement	Minimum 12 years from date of report
Accident reporting	HSE requirement	Adults – 6 years from date of incident Children – until the child attains 25 years of age
Fire precaution log books	HSE requirement	6 years
Records of tests and examinations of control systems and protection equipment under COSHH	HSE requirement	5 years from date of report
Pupil Records		
Admissions records (SIMS)	HS and progress tracking	Retained while on roll plus 1 year
Free school meals records	Audit requirement	6 years from the tax year they relate to
Attendance records	Safeguarding & Welfare	Retained while on roll plus 1 year
SEN records	Welfare & Progress	Forwarded to child's new school
Child protection records	Welfare & Progress	Forwarded to child's new school (separately from main record) Copy held in school until child attains 25 years of age
Pupil file (paper)	HS, Welfare & Progress	Forwarded to child's new school
Assessment records	Assessment reporting	Retained while on roll plus 1 year

Appendix D: Data Protection Guidance for Teachers

Data Type (What & Who)	Service & Location (Where)	Risks	Action
Assessment & contextual data of children	T: shared drive (progress trackers & import data) Memory Sticks Paper copy (assessment & dashboard) Markbooks (digital & paper)	Loss of data Access to information from unauthorised personnel, eg parent at consultation evening or child through display on whiteboard / hard copy on teacher's desk	Use of encrypted usb stick whenever data is taken from the main system Files never left open on classroom computer Check white-board (use freeze or turn off if using computer during teaching time)
Behaviour File with names of children & description of behaviour	Record of RA meetings & behaviour chronology in behaviour file in classroom Record of internal isolation & exclusion (hard copy HT office)	Access to information from unauthorised personnel, eg parent at consultation evening	Folder to be out of public view at all times
Behaviour Log containing list of children	Hard copy in classroom (teacher's desk)	Access to information from unauthorised personnel, eg child during school day / after school club or parent at consultation evening	Sheets / folder to be out of public view during non-teaching hours
Positive Behaviour Plans	Hard copy held by child - usually on teacher's desk during lessons and may be carried by child.	Loss of card containing general behaviour progress and teacher comments	Ensure comments are professional & positive Cards to be out of public view at non-teaching times
Attendance information	Online - eschool Hard copy of reports to Year Leaders / Class Teachers	Information accessed by unauthorised persons, eg pupils through public display on whiteboard or parents at consultation	Online register not to be shared on whiteboard Minimise eschools when not in use and log-out when computer is not attended File hard copy of attendance reports in behaviour file
Health, personal & family info	Letters in behaviour file Letter in pupil file Emails	Access to information from unauthorised personnel, eg parent at consultation evening	Correspondence filed in behaviour file or main pupil file at school office (files not in public view) Emails minimised and log-out when computer is not attended Check state of white-board (use freeze or turn off if using computer during teaching time)
Seating plans (ability / behaviour / needs)	Hard copy on teacher's desk	Information accessed by unauthorised persons, eg parents at consultation	Seating plan to be out of public view during non-teaching time
Data on portable devices	Laptop or USB stick	Loss of laptop / USB stick	Laptop password protected Encrypted sticks used
Medical Information	Class medical boxes Class folder	Information accessed by unauthorised persons, eg parents at consultation	Medical boxes and files kept out of public view at non-teaching times
Exercise books	Classroom Teacher's home	Information accessed by unauthorised persons, eg parents at consultation or public in case of loss of books	Books not to be left in vehicles

Appendix E: Guidance for Home Working

Purpose

There may be times when it is appropriate to take data away from the school site. This may include, but is not limited to, the analysis of assessment data, the writing of school reports or training courses. Due regard must be given to the protection of data in all such cases.

Risks

There are inherent risks in the removal and transportation of data, including:

- loss of data through error, negligence or theft;
- deletion of data through error;
- data breach through unauthorised access;
- corruption / loss of data through malfunction, malware or virus.

Safeguards

Simple safeguards should be employed each time data is taken away from the school site, including:

- The use of the encrypted USB stick issued to teachers;
- The use of school or personal computers only (not a public computer);
- Not using public wifi whilst accessing data;
- Checking that devices have up-to-date security / firewalls in place to prevent outside access;
- Ensuring that written passwords to files, portable devices and computers are not kept with them;
- Only taking the data that is essential to the task (anonymise documents if practicable);
- Work in an appropriate environment;
- Ensuring that equipment & data is not left unattended;
- Limiting the possibility of 'over the shoulder' viewing (set screen saver to 60 seconds);
- Only using school email addresses.

Concerns

Any concerns relating to a loss or breach of data should be reported to the Headteacher or School Business Manager as soon as is practicable.

Appendix F: Process for dealing with Data Breach / Loss

Purpose

This breach procedure sets out the course of action to be followed by all staff at Wendover CE Junior School if a breach / loss of data takes place.

1. After becoming aware of the breach, the processor will **notify the controller** without undue delay.
 2. The controller 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 controller will **inform the Chair of Governors and other agencies** as necessary, eg police or social care. Where it is likely that the breach will result in a risk to the rights and freedoms of subjects, the supervisory authority will be informed within 72 hours (if longer, or where information is reported in phases, the reason for delay will be given) and shall at least:
 - (a) describe the nature of the personal data breach including the categories, number of data subjects and records;
 - (b) communicate the name and contact details of where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures necessary to mitigate its possible adverse effects.
 4. The controller will take steps to **recover losses and limit damage**. This might include:
 - (a) attempting to recover lost equipment.
 - (b) contacting the Local Authority and brief staff, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual(s) concerned (in the event of an enquiry, obtain the enquirer's name and contact details and promise a return call; report the call to the headteacher / controller).
 - (c) contacting the Local Authority Communications Officer on 07825 430978
 - (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) change to entry codes or IT system passwords as appropriate and inform staff.
 5. In most cases, an **investigation** will be conducted by the headteacher to ascertain the data involved, potential effect on the subject and steps to remedy the situation. In particular, it should consider:
 - (a) the type of data and level of sensitivity
 - (b) how data was breached and effectiveness of protection currently in place
 - (c) what happened to the data and how it may be used
 - (d) how many / type of subjects that might be affected and wider consequences
- A clear record of finding and actions should be made and communicated to the relevant authority (ICO).
6. People / agencies may need **notification** of the breach after the investigation. Information should include a description of the breach (when, how and what) and actions taken to mitigate the risk. Specific clear advice should be given to individuals about how they can protect themselves and what the school can do to help. They should be given the opportunity to make a formal complaint if they wish.
 7. A **review** of findings and procedures should be reported to senior leaders and governors. Consideration will be given to the need for change to the procedures and / or disciplinary action.
 8. **Implementation** of this procedure will be through induction and regular updates to staff.