Sponsor	**DFO**
Issue Date	**July 2019**
Next Review Date	**June 2020**
Committee	**Estates**

DATA PROTECTION POLICY

Contents

1. Data Protection Principles

The Data Protection Act 2018 incorporating the General Data Protection Regulations [GDPR] is based on data protection principles that our school must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

2. Collecting Personal Data

2.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 5 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone against identity theft or protect their reputation
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

2.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Data Retention and Storage Policy.

3. Sharing Personal Data

We only share personal data with others to fulfil our contractual and legal obligations, if we have a legitimate interest as described in our Privacy Notice or we have gained explicit consent to do so. Examples of when we may share data are:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, catering contractors and travel companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- The school may use a third party to gather information about individuals from publicly available sources – for example, Companies House, the Electoral Register and the media – to help understand more about the individual and their ability to support us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Who Does What

4. The Data Controller

Woldingham School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore Woldingham School is a data controller.

Woldingham School is registered as the data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

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

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations and has a nominated role responsible for Data Protection.

5.2 Privacy Officer

The Privacy Officer (PO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The PO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the PO's responsibilities are set out in their job description.

Our PO is currently Simon Hopkins and is contactable via privacy@woldinghamschool.co.uk or 01883 654202.

5.3 Director of Finance and Operations [DFO]

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the PO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether, or not, they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Annex D.

7. Training

All staff and governors are required to undertake data protection training as part of their induction process and then annually to stay up to date with any changes to Data Protection law and school policies.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

8. Links with other policies

This data protection policy supports our other policies including:

- Safeguarding and Child Protection policy
- ICT Acceptable Use (Staff) policy
- ICT Acceptable Use (Student) policy
- Admissions policy
- Data Retention and Storage policy
- Recruitment, Selection and Disclosure policy
- Security, Access, Workplace Safety and Lone Working policy

Annexes

A. Legal Considerations
B. Access to Information.
C. Technical Considerations.
D. Data Breach Management Plan.

Annex A

Legal Considerations

1. Aims

Woldingham School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Family Circumstances • Sex life or sexual orientation
Processing	Anything done to personal data (including photographic images and video), such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Annex B

Access to Information

1. Subject access requests and other rights of individuals

1.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing to the Privacy Officer [PO]. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the PO.

1.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

1.3 Responding to subject access requests
When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

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

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

1.4 Other data protection rights of the individual
In addition to the right to make a subject access request (see paragraph 1.1), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the PO. If staff receive such a request, they must immediately forward it to the PO.

2. Parental requests to see the educational record

Parents, or those with parental responsibility, can request access to their child's educational record (which includes most information about a student) by applying in writing to the Deputy Head Academic.

There is no legal obligation to supply the educational record but we will, unless there are special circumstances, aim to respond with the data within 15 school days from the receipt of the request.

Annex C

Technical Considerations

1. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to register attendance), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can use a PIN code on the registration devices.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

2. CCTV

We use CCTV and Automatic Number Plate Recognition [ANPR] technology in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DFRO.

3. Photographs and videos

In the normal day to day operation of the school we use photographic and video images of students and staff regularly, including to celebrate achievements at events and performances, provide a visual record of events and performances and to use in marketing materials.

Other uses may include:

- Internal identification purposes

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages, including streaming of events.

Unless they have indicated to the contrary on the Form of Acceptance, parents consent to the school making use of their daughter's photograph or image to feature in school communications and promotional materials whilst the girl is at the school and after she has left the school. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. Parents who do not want their daughter's photograph or image to appear in any of the school's promotional material must make sure their daughter is also well aware of this fact.

In the case of media coverage where full names and images are required, the school will request parental permission to use imagery, full name and area of residence.

The school may use photography and video to record key school events in which images of parents may feature. These are disseminated to parents and alumnae and may be used for promotional purposes. Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

- Parents should be mindful of the need to use their cameras with consideration and courtesy for cast members or performers on stage and the comfort of others.
- Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts.
- Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.
- The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase.

USE OF CAMERAS AND FILMING EQUIPMENT BY PUPILS

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff. The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset. The misuse of images, cameras or filming equipment in a way that breaches this policy, or the Anti-Bullying Policy, or the Acceptable Use of Technology Policy, is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

See our Safeguarding and Child Protection policy, ICT Acceptable Use policies, Media Relations policy and the Social Media policy for more information on our use of photographs and videos.

4. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Privacy Officer [PO], and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see Annex A)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the PO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Annually training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - ***For the benefit of data subjects*** – we will make available the name and contact details of our school and PO. We will also make available information about how we use and process their personal data (via our privacy notices)
    - ***For all personal data that we hold*** – we will maintain an internal record of the type of data we hold, who we hold that data about and how and why we are using the data. In addition, we will record any third-party recipients, how and

why we are storing the data, retention periods and how we are keeping the data secure

5. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office. E.G. printed information used on school trips
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Information Security policy for further information)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

6. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Annex D

Data Breach Management Plan

Policy Statement

Woldingham School holds personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This Data Breach Management Plan applies to all personal, sensitive and special category data held by Woldingham School. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose

This Data Breach Management Plan sets out the course of action to be followed by all staff at Woldingham School if a data protection breach takes place. This Plan is invoked as part of the School Emergency Response Plan and will therefore be overseen by the School Emergency Management Team [SEMT] in conjunction with the Privacy Officer [PO].

Legal Context

The Data Protection Act 2018, including the General Data Protection Regulations [GDPR], makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the Data Protection Act covered by Article 5 of the GDPR states that organisations must ensure that Personal data shall be:

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of student, parent, alumnae, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment or software failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- Malware and phishing scams where information is obtained by deception.

Immediate Containment/Recovery

On discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the PO or, in their absence, either the DFO or another member of SLT. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The PO (or nominated representative) will inform SLT and the School Emergency Response Plan will be initiated.

3. A clear record should be made of the nature of the breach and the actions taken to mitigate it on a Woldingham School Data Breach Reporting form, see ***Appendix 1*** for the form. The form in ***Appendix 4*** should be used to record the timeline of actions taken throughout this process.

4. The following steps are a summary of the recommended actions to follow after becoming aware of a possible data breach. The SEMT must be kept informed of all actions undertaken by the PO (or nominated representative). A more detailed checklist can be found in ***Appendix 3***.

5. The PO (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 Operations Manager.

6. The PO (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. However, should the PO (or nominated representative) require any expert guidance and assistance; they can contact the Information Commissions Office helpline on 0303 123 1113 or via live chat on the ICO website (ico.org.uk).

7. The PO (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. ***Appendix 2*** contains a table to assist with the evaluation of incident severity.

8. The PO (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 relevant third parties affected, such as banks and other service providers, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned.

c. 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 PO (or nominated representative).

d. Contacting the Marketing team so that they can be prepared to handle any press enquiries.

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

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

g. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the PO (or nominated representative) to fully investigate the breach. The PO (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 are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (students, parents, staff members, suppliers etc) and whether there are wider consequences to the breach.

The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The PO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach.

In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the conclusion of the investigation.

Every incident should be considered on a case by case basis. The following points will help SEMT to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious consequences due to the loss of personal, sensitive or special category data the PO should notify the ICO. There is guidance available from the ICO and the first stage should be contacting their Helpline 0303 123 1113 as they will verify whether the incident is reportable and advise on next actions.
- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure).

Review and Evaluation

Once the initial aftermath of the breach is over, the PO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available SLT meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This Data Breach Management Plan may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this Data Breach Management Plan whenever the data protection policy is reviewed.

Implementation

SLT should ensure that staff are aware of the Data Protection policy and its requirements including this Data Breach Management Plan. This should be undertaken as part of induction and supervision. If staff have any queries in relation to the policy, they should discuss this with their line manager or the PO.

Appendices:

1. **Data Breach Reporting Form**
2. **Evaluation of Incident Severity**
3. **Data Breach Checklists**
4. **Timeline for Incident Management Form**

Appendix 1: Data Breach Reporting Form

Description of the Data Breach:	
Time and Date breach was identified and by whom.	
Who is reporting the breach: Name/Post/Dept	
Contact details: inc telephone and email	
Classification of data breached i. Public Data ii. Personal Data iii. Sensitive Data iv. Special Category Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	
Lessons learnt / improvements identified	

Email form to the Privacy Officer: privacy@woldinghamschool.co.uk
Call 01883 654202 and advise the PO that a Data Security Breach report form is being sent.

Received by:	
Date/Time:	

Appendix 2: Evaluation of Incident Severity

The severity of the incident will be assessed based upon the following criteria:

High Criticality: Major Incident	**Contact:**
• Special Category/Sensitive Data • Personal data breach involves > 1000 individuals • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures ***Example*** ***School MIS database compromised*** ***Pupil medical records lost*** ***Staff HR and Payroll data sent in error***	Lead Responsible Officer • As defined in the School Emergency Response Plan. Other relevant contacts • Chair of Governors, Headmistress and Communications lead • Internal Heads of Year / Heads of Departments as required • Contact external parties as required i.e. police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Personal Data • Not contained within Woldingham School • Breach involves personal data of more than 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response • Incident response may require notification to Board of Governors and SLT ***Example*** ***Pupil contact information lost on school trip*** ***All WPSA email addresses visible in bulk email outside of school community***	Lead Responsible officer • Privacy Officer Other relevant contacts: • Chair of Governors, Headmistress and Communications lead • Internal Heads of Year / Heads of Departments • Head of Human Resources • Head of Operations • Head Caretaker/Security • Director of IT
Low Criticality: Minor Incident	**Contact:**
• Internal or Personal Data • Small number of individuals involved • Risk to Woldingham School low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours ***Example:*** ***Email sent to wrong recipient*** ***Loss of encrypted device***	Lead Responsible Officer • Privacy Officer Other relevant contacts: • Director of IT to advise and lead on technical aspects of containment / recovery • Internal Heads of Year / Heads of Departments • SLT to follow up on policy and procedures for managing personal data breaches

Appendix 3: Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Privacy Officer [PO] to coordinate the evaluation of the incident severity.	**See Appendix 2**
2	PO to ensure responsibility taken or delegated for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. In the event that the breach is severe, the School Emergency Response Plan will be executed.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the PO or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	

B	Assessment of Risks	To identify and assess the ongoing risks that may be associated with the breach.
7	What type and volume of data is involved?	Data Classification/volume of individual data etc
8	How sensitive is the data?	Special category data or sensitive data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
9	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
11	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
12	How many individuals' personal data are affected by breach?	
13	Who are the individuals whose data has been compromised?	Students, parents, applicants, staff, customers, clients or suppliers?
14	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

C	Consideration of Further Notification	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
18	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
19	Can notification help Woldingham School meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
21	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the PO).	Contact and liaise with the Headmistress and the Board of Governors.
22	Consider the dangers of 'over notifying'.	Not every incident will warrant notification, i.e. notifying the whole school community of an issue affecting only one year group may well cause disproportionate enquiries and work.
23	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).

24	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

D	**Evaluation and Response**	**To evaluate the effectiveness of the University's response to the breach.**
26	Establish where any present or future risks lie.	
27	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
28	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
29	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
30	Report on findings and implement recommendations.	Report to SLT and Board of Governors.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority