Wychwood School
OXFORD

# DATA PROTECTION POLICY
# Author: AKJ
# Inception: March 2018
# Review: February 2021
# Date of next review: February 2023

Wychwood School will check the Information Commissioner's Office (ICO) website at each review date to ensure the Data Protection policies are up to date.

https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/

**PRINCIPLES**
This policy is based upon the eight data protection principles from the Data Protection Act 1998 and reiterated in the General Data Protection Regulation (GDPR) and draft Data Protection Act 2018. These rules for 'good information handling' are:

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Rights Under The General Data Protection Regulation (GDPR) and the Data Protection Act 2018**
Individuals or data subjects are entitled to the following rights under GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The Right to be Informed

- We provide individuals with all the following privacy information:
- The name and contact details of our organisation (See Privacy Notices)
- The contact details of our data protection compliance lead (See Privacy Notices)
- The purposes of the processing (See Privacy Notices)
- The lawful basis for the processing (See Privacy Notices)
- The legitimate interests for the processing (See Privacy Notices)
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to) (See Privacy Notices)
- The recipients or categories of recipients of the personal data (See Privacy Notices)
- The details of transfers of the personal data to any third countries or international organisations (if applicable)
- The retention periods for the personal data (See the Data Requesting, Storage, Retention and Disposal Policy)
- The rights available to individuals in respect of the processing (see this Policy and Privacy notices)
- The right to withdraw consent (if applicable) (see this Policy and Privacy notices)
- The right to lodge a complaint with a supervisory authority (See Privacy Notices)
- The source of the personal data (if the personal data is not obtained from the individual it relates to)
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to) (See Privacy Notices)

**The Right of Access**

Individuals have the right to access their personal data and supplementary information (see this Policy). The right of access allows individuals to be aware of and verify the lawfulness of the processing. An individual can make a request for access verbally or in writing to Wychwood, Oxford and the request will be dealt with under this Policy. This request will be logged.

**The Right to Rectification**

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing to Wychwood, Oxford and the request will be dealt with under this Policy. This request will be logged.

**The Right to Erasure**

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. An individual can make a request for erasure verbally or in writing to Wychwood, Oxford. The right is not absolute and only applies in certain circumstances. A right to erasure request will be dealt with under this Policy.

The right to erasure of personal data applies under the following circumstances if:

- the personal data is no longer necessary for the purpose which Wychwood, Oxford originally collected or processed it for
- Wychwood, Oxford is relying on consent as the lawful basis for holding the data, and the data subject withdraws their consent

- Wychwood, Oxford is relying on legitimate interests as the basis for processing, the data subject objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- Wychwood, Oxford is processing the personal data for direct marketing purposes and the data subject objects to that processing
- Wychwood, Oxford has processed the personal data unlawfully
- Wychwood, Oxford has to erase data to comply with a legal obligation
- Wychwood, Oxford has processed the personal data to offer information society services to a child.

Wychwood, Oxford recognises the emphasis placed on the right to have personal data erased under the GDPR if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments. Therefore, Wychwood, Oxford will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- for the establishment, exercise or defence of legal claims

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices)
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

Wychwood, Oxford will refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Where the School considers that a request is manifestly unfounded or excessive the School can either request a "reasonable fee" to deal with the request or refuse to deal with the request. Each case will be dealt with on a case-by-case basis and the decision will be justified, communicated to the data subject making the request and recorded.
If the decision is taken to charge a fee, then the amount charged will be based on the administrative costs of complying with the request and this will be communicated to the data subject. In these cases, the School will not comply with the request until we have received the fee.

**Right to Restrict Processing**

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and applies only in certain circumstances. When processing is restricted, the School is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. These requests will be logged.
The right to restrict processing of personal data applies in the following circumstances:

- the individual contests the accuracy of their personal data and the School is verifying the accuracy of the data;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- Wychwood, Oxford no longer needs the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim
- the individual has objected to you processing their data under Article 21(1) of the GDPR, and the School is considering whether our legitimate grounds override those of the individual.

Wychwood, Oxford will restrict processing by making the data on the MIS unavailable to users and by removing paper files to the Head's office and retaining them in the lower locked drawer of the Child Protection filing cabinet.
Restricted data will not be processed in any way **except to store it** unless:

- the School has the individual's consent
- it is for the establishment, exercise or defence of legal claims
- it is for the protection of the rights of another person (natural or legal)
- it is for reasons of important public interest.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that the individual has disputed the accuracy of the personal data and the School is investigating this; or the individual has objected to the School processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of the School's legitimate interests, and the School is considering whether our legitimate grounds override those of the individual. Once the School has made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, the School may decide to lift the restriction. In this case, the School will inform the individual **before** we lift the restriction.

Wychwood, Oxford will refuse to comply with a request to restrict processing if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
Where the School considers that a request is manifestly unfounded or excessive the School can either request a "reasonable fee" to deal with the request or refuse to deal with the request. Each case will be dealt with on a case-by-case basis and the decision will be justified, communicated to the data subject making the request and recorded.
If the decision is taken to charge a fee, then the amount charged will be based on the administrative costs of complying with the request and this will be communicated to the data subject. In these cases, the School will not comply with the request until we have received the fee.

**Right to Data Portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal

data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
The right to data portability only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

This is unlikely to apply to Wychwood where no data processing is carried out by automated means.

**Right to Object**
The School must inform individuals of their right to object "at the point of first communication" which is in the various privacy notices and in these the right to object is "explicitly brought to the attention of the data subject and is presented clearly and separately from any other information".

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

However, such individuals must have an objection on "grounds relating to his or her particular situation". If a data subject makes an objection then Wychwood, Oxford will stop processing the personal data unless:

- the School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

If a data subject objects to processing personal data for direct marketing purposes, Wychwood, Oxford will stop such processing immediately. Should data subjects wish to object online, the website offers an opportunity for them do so directly.

**Rights related to automated decision making including profiling**
The GDPR applies to all automated individual decision-making and profiling. Wychwood, Oxford does not undertake any automated individual decision-making or profiling.

**Recognition of Requests**
The GDPR does not specify how to make a valid request for rectification, erasure or to restrict processing. Wychwood, Oxford recognises that an individual can make these requests verbally or in writing and that they can also be made to any part of the School and does not have to be to a specific person or contact point. A request for rectification **does not** have to include the phrase 'request for rectification' or mention Article 16 of the GDPR. A request for erasure **does not** have to include the phrase 'request for erasure' or Article 17 of the GDPR. A request for restriction of processing **does not** have to include the phrase 'request for restriction of processing' or mention Article 18 of the GDPR.

This presents a challenge as any of the School's employees could receive a valid verbal request. The School has a legal responsibility to identify that an individual has made a request to us and to handle it accordingly. Therefore staff who regularly interact with individuals will be given specific training to identify a request. If the School believes a

request has been received then we will check with the requester that we have understood their request, as this can help avoid later disputes about how you have interpreted the request. All requests and their nature and details will be recorded in the appropriate Requests logs.

**Disclosure of Personal Data to Others and Requests**

Where personal data has been disclosed to others, and there is a request for rectification, erasure or to restrict processing, Wychwood, Oxford will contact each recipient and inform them of the actions taken with respect to the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

**COMPLAINTS**

Where a data subject is concerned about the Wychwood, Oxford's response to any Data Protection issue, we request that they raise their concern with us in the first instance. Alternatively, data subjects can complain at any time about how the school has handled their data: they can contact the Information Commissioner's Office at https://ico.org.uk/concerns/ and the Information Commissioner Office's (ICO) helpline is 0303 123 1113.

**CONSENT**

We ask parents to give consent for the processing of their daughter's personal and special data on their behalf by signing the Acceptance Form having read the Terms and Conditions on entry to Wychwood, Oxford. We ask staff to give consent for the processing of their personal and special data by signing their contract at the beginning of their employment with Wychwood, Oxford.
Other consents are requested via the New Girls' Pack.

**DATA BREACHES**

A data breach is a security incident that has affected the confidentiality, integrity or availability of personal data: i.e. a data breach results in confidential data potentially being viewed, used or downloaded by an entity that is not authorised to do so; or if personal data is lost, destroyed, corrupted or disclosed; or if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If a member of staff is responsible for or discovers a data breach, they are required to tell the Head immediately. The following are NON-EXHAUSTIVE examples of data breaches

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a processor or handler
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.
- loss or theft of pupil, staff or governing body data
- Inappropriate access controls allowing unauthorised use

- equipment failure
- poor data destruction procedures
- human error
- cyber-attack
- hacking

The procedures to be followed in managing a data breach are to be found in Appendix A.

**DATA HANDLERS AT WYCHWOOD**

The data handlers at Wychwood are identified as

| | |
|---|---|
| Admissions and Departures | Lead: Marketing and Admissions Manager |
| Marketing and Communications | Lead: Marketing and Admissions Assistant |
| Medical Data | Lead: Junior Housemistress and School Nurse |
| Alumnae | Lead: Marketing and Admissions Manager |
| Finance | Lead: Bursar and Finance Assistant |
| General | Lead: Office Manager and Administrative Assistant |
| Pastoral | Lead: Deputy Head and form teachers, progress tutors, house staff, catering team, cleaning staff and Senior Pastoral Team (SPT) |
| Education | Lead: Director of Studies and specialist teachers, form teachers and progress tutors |
| Discipline | Lead: Head and form teachers, progress tutors, Senior Leadership Team (SLT) |
| Incidents and Accidents | Lead: Bursar and medical staff, sports teacher, Gap Assistants, form teachers, Bursar and facilities staff |
| Safeguarding | Lead: DSL |
| SEND and SEMH | SENDCo |

Every member of staff is regarded as a data handler in some area of school and boarding life. Data processing training will be done during staff induction and repeated on a three year cycle. Staff will be required to attend the next three yearly training event after they arrive in school, regardless of whether it is less than three years since they were trained and thereafter to maintain the three year training cycle. Records will be kept in the Training Register – All Staff Whole School Training.

**INFORMATION SHARING AND DISCLOSURE**

We do not rent, sell or share personal information about anyone associated with Wychwood, Oxford with other people or non-affiliated companies except to provide products or services requested with consent from the individuals concerned.

We will use reasonable efforts to ensure that personal data is not disclosed to regional/national institutions and authorities, unless required by law or other regulations.

**INSPECTION**

The Independent School Inspectorate (ISI) inspectors are likely to see some personal data while they are on Wychwood's premises, they do not collect that data for removal from the school site nor retain it. In that sense, they do not routinely process personal data. ISI states that 'When it is necessary to include personal data in an evidence base, usually in exceptional circumstances, then it will be kept securely and uploaded for safekeeping to the ISI system, after which it will be deleted in due course in accordance with the ISI Data Protection/Retention policy.' *ISI Updates to Schools May 2018*

**ORGANISATIONS WITH WHOM WE ROUTINELY SHARE DATA**

This data can be staff data or pupil data depending on the organisation.
Atlantic Data, BSA, AtoZ, CEM centre, DfE, DBS, Dr's surgery, DofE, the examination boards, FoW, GL Assessment, GSA, Halsey Travel, HMRC, Home Grown Media, Home Office, ISC, ISI, JCQ, MCC, Marsh Insurance, NS Optimum, OSBP, OSCB, People's Pension, TP, WA, UCAS, UK Visas & Immigration (UKVI): Home Office, WCBS, YE,

**PASSWORDS**

The Wychwood, Oxford network will remember staff and pupils' password history for the last 20 passwords. This means a password that has already been used cannot be repeated within the next 20 passwords.
The maximum password age will be 180 days and the network will require operators to change passwords every 180 days.

The minimum password length will be 8 characters with the following complexity requirements: passwords must:

- not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- be at least 8 characters in length
- contain characters from all four of the four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

**PRIVACY NOTICES**

Wychwood provides Privacy Notices for Alumnae, Parents, Pupils under 13, Pupils over 13, and Staff. These can be found on the school website under Policies.

- Each Privacy Notice will be reviewed and updated annually, to ensure it still accurately reflects the school's use of personal data.

- Each Privacy Notice will be re-issued to all those affected when substantial amends have been made.

- All data subjects will be provided copies of the Privacy Notice either before the school begins processing their personal data, or within a reasonable time (and not more than one (1) month) thereafter (this will include existing parents, pupils and staff and alumnae etc.).

**PUBLICATION OF EXAMINATION RESULTS**

This is dealt with under the Publication of Examination Results Policy. Parents and pupils are assumed to give permission for the school to use their examination results as described in the policy. They may opt out by contacting the Head.

**USE OF SCHOOL ICT**

Staff dealing with sensitive personal data will not use computers to which girls have access. They will not process such data in rooms where the computer screen may be visible to others.

**SUBJECT ACCESS RIGHT**

Both the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR) provide for a right enjoyed by all individuals – including parents, pupils, staff (past, present and prospective) – to know what personal data about them is being held and used by organisations (including schools), and broadly for what purpose, where it came from, and who else might receive it. This is known as the Subject Access Right or SAR. Wychwood, Oxford will aim to treat any SARs according to the Information Commissioner's Office "Subject Access Code of Practice". Usually, individuals are also entitled to a "permanent copy" of the personal data held. The SAR right is wide in scope and has no time limitation. Wychwood, Oxford recognises that while fulfilling a SAR will incur considerable time and costs, from 25 May 2018 no charge can be made in most cases.

Children have exactly the same rights to make a SAR as adults, and, strictly speaking, those rights belong to the child (and not the parent). However, a person with parental responsibility would normally exercise those rights on behalf of a child too young to understand the nature of the request (usually taken to mean under twelves). A child of any age can also ask a parent or third party to make a SAR on their behalf.

Wychwood, Oxford notes that the SAR is **not** the same as a parent's statutory right to receive a copy of their child's educational record under the Education Act 1996, which is sometimes cited by parents but which **does not apply** to independent schools.

**Personal Data**

The definition of personal data is wide and includes correspondence, emails, minutes, reports, results, databases, lists and expressions of opinion. As Wychwood, Oxford has close relationships with pupils and parents, a good deal of personal data of this kind will be accumulated over the career of a pupil.

**Repetitious Requests**

Only repetitious requests, without allowing a reasonable time since the previous SAR, can safely be ignored.

**Making a Valid SAR**

A SAR submitted to Wychwood, Oxford:

- must be made in writing, including online, and it must make clear the requester wishes to access information about themselves held by the school.
- can be made to anyone in the organisation.
- can be made on another's behalf provided Wychwood, Oxford is satisfied that the third party is genuinely acting on the individual's behalf – for example, by their solicitor, or a family member.

The SAR does not have to mention the DPA or GDPR.

**Response to a SAR**

Wychwood, Oxford will request any information we reasonably require to confirm the identity or authority of the requester, or in order to locate the data sought (if this is not immediately obvious, with e.g. CCTV footage), before responding formally. This request will be made in writing.

If there is any doubt, Wychwood, Oxford will request a direct or signed "authority" from the individual (e.g. the pupil) especially if there is a parental request about a pupil.

The GDPR and Data Protection Act 2018 require a response to a SAR **within a calendar month**, starting with the date on which the SAR is received or the date on which the identity confirmation or authority confirmation is received, whichever is the latest.

Once the confirmation information requested is received, Wychwood, Oxford will respond to the data subject in writing, referring them to the Data Protection policy, defining personal data, explaining the process, outlining the grounds on which a request can be refused and setting out a time scale. Wychwood, Oxford will aim to keep the data subject informed of progress through the process.

**Process of Preparing the Response to a SAR**

All electronic systems under the school's control, which may include personal devices or email accounts where used on school business (by e.g. peripatetic music teachers or directors), and any "filing system" as defined by the GDPR will be searched.

Under the DPA 1998, SARs included hard copy records only to the extent they were sufficiently well-organised to give easy access to specific information about an individual – i.e. a “filing system”. ICO Guidance is yet to be issued on the GDPR interpretation of “filing systems” (April 2018).

The GDPR suggests that "manifestly unfounded or excessive" requests can be ignored or fairly charged for.

**Content of a SAR**

A SAR only provides access to the individual's own "personal data". Case law suggests that this is widely defined to include anything that "relates to" an identifiable, living individual (which means it includes initials, nicknames, job titles etc.). All the same, it is worth remembering that the right only relates to personal data, not whole documents. An entire email chain will not always be personal data of someone mentioned in the subject line, for example.

Some requesters will expect full document disclosure of anything of interest to them: however, where documentation is factual or procedural or relates to the complaint being made and does not relate to the data subject making the SAR’s personal data, this does not need to be disclosed.

Where personal data about the person making a SAR also constitutes "personal data" about another person (a "third party"), Wychwood, Oxford is **not obliged** to disclose this mixed data in response to a SAR unless either (a) the third party has consented or (b) it is "reasonable", taking into account all the relevant circumstances, to disclose without consent. In such cases information may be redacted.

Wychwood, Oxford's policy is to disclose as much of the requester's personal data as they can without unreasonably identifying the third party, while remaining aware that disclosure of information which also relates to a third party may give rise to a breach of confidence or data protection towards that third party.

Other factors to be considered will include the third party's views, any harm or distress that may come to them, and their expectations of confidentiality.

Under the current draft DPA 2018, it will always be assumed reasonable to disclose where that other person is a social worker or education worker, which latter definition will include from 25 May 2018 teachers (and other staff) of an independent school.

**Delivery of the SAR to the Data Subject**

The format in which the SAR information will be delivered to the data subject will depend on the type of information the SAR response contains: it could be compiled in a table or single document, or scanned or photocopied from originals and sent digitally or by hard copy.

Wychwood, Oxford will take great care to ensure the SAR response is delivered securely with effective redactions). In order to effect safe delivery, Wychwood, Oxford will contact the data subject to agree a time and method with the requester.

Thought will be given to the suitability of delivery in a case-by-case basis, which will, in turn, depend on the sensitivity, volume and nature of the data. Post, even by recorded delivery, is less secure than a courier, which in turn is less secure than collecting or delivering in person. Ordinary email is less secure than an encrypted transfer. The delivery method of CCTV footage is particularly sensitive and Wychwood, Oxford will offer to show the data subject footage on-site first before any type of delivery is considered.

**Exemptions to the Subject Access Right**

Information may be exempt from disclosure if it:

- is *legally privileged*
- records the intentions of the school in *negotiations* with the individual making the SAR;
- consists of a *confidential reference* given by the school (though not currently confidential references received by the school)
- consists of *exam or test answers* or *exam results* before the allotted publication time;
- is held for purposes of *management planning* (e.g. redundancy planning)
- would prejudice the prevention and detection of *crime* if disclosed (e.g. in live investigations)
- might cause serious harm or distress in limited *social work* contexts.

**SECURE DISPOSAL**

Wychwood, Oxford undertakes to dispose of all confidential, sensitive or personal information securely. This means the information must end up in a condition where it cannot either be read or reconstructed.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Electronic communications should be deleted, then deleted from the Deleted Box.

Skips and 'regular' waste disposal are not considered secure.

Wychwood, Oxford ensures that we receive a Secure Disposal Certificate each time we use third party disposal experts.

**WEBSITE PRIVACY STATEMENT**

The Website Privacy Statement is maintained as a separate entity: please see this in Current Policies

**This policy does not apply to the practices of companies that Wychwood, Oxford do not own or control, or to people that we do not employ or manage.**

**Appendix A – MANAGING A DATA BREACH**

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

**Initial assessment, containment and recovery – first few hours:**

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

2. The Head 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. Questions to ask include:

- *How long has the breach been active, what data was involved and how far has it got?*
- *What immediate steps can be taken to prevent it going further? Consider:*
  - *if a cyber breach, involve the school's IT personnel from the outset;*
  - *if human actor(s) are involved, can they be contacted to give reassurances;*
  - *if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;*
  - *are specialists needed: forensic IT consultants, crisis management PR, legal etc.*

3. The Head must inform the Chair of Directors as soon as possible. As a registered Data Controller, it is the School's responsibility to take the appropriate action and conduct any investigation.

4. The Head 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.

Ongoing assessment of risk and mitigation – first 72 hours (and initial notification where required): Questions to ask include

- *Build up a more detailed picture of the risk and reach of the security breach:*
  - *how many have been affected?*
  - *was any sensitive personal data involved – health, sexual life, crime?*
  - *was financial data involved and/or is there a risk of identify fraud?*
- *Identify if a crime has been committed and involve police or cyber fraud unit.*
- *Assess if insurers need notifying (major loss, crime, or possible legal claim(s))*
- *Decide if the likely risk of harm to the data subjects:*
  - *is sufficient to require a full or preliminary notification to the ICO; and*
  - *is sufficiently serious to require communication to affected individuals*
- *If not, is this a matter we can document but deal with internally?; or*
- *If so, what can we usefully tell the ICO and/or individuals at this stage?*
  - *e.g. provide fraud or password advice, offer counselling etc.*

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

a. Attempting to recover lost equipment.

b. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head.

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

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

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

**Ongoing evaluation, monitoring and remediation:**

1. Continue to monitor and assess possible consequences (even if apparently contained).
2. Keep the ICO and/or those affected informed as new information becomes available.
3. Tell the ICO and/or those affected what you are doing to remediate and improve practice.
4. Begin process of review internally:

- how did this happen? What could we have done better?
- would training or even disciplinary action be justified for staff members?
- were our policies adequate, and/or adequately followed?
- if our contractors were involved (e.g. systems providers), did they respond adequately and do we have any remedies against them if not?

**Investigation**

In most cases, the next stage would be for the Head to investigate the breach fully. The Head should ascertain whose data was involved in the breach, the potential effect on the data subject(s) and what further steps need to be taken to remedy the situation. The investigation should consider:

- the type of data
- its sensitivity
- what protections were in place (e.g. encryption)
- what has happened to the data;
- whether the data could be put to any illegal or inappropriate use
- how many people are affected
- what type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

**Record keeping and putting outcomes into practice:**

A clear record should be made of the nature of the breach and the actions taken to mitigate it.

1. Keep a full internal record, whether or not the matter was reported or resulted in harm.
2. Log this record against wider trends and compare with past incidents.
3. Make sure all past outcomes were in fact put into practice.
4. Ensure any recommendations made by, or promised to, the ICO are actioned.
5. Notify the Charity Commission as an RSI, if a charity, at an appropriate juncture.
6. Review policies and ensure regular (or specific, if required) training is actually completed.

**Notification**

Some people, agencies or contractors may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head should, after seeking expert or legal advice, decide whether anyone is to 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 breach. Every incident should be considered on a case by case basis. A data breach should be reported if the breach will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The ICO can be notified using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Or, the ICO can be notified using the security breach notification form, which should be sent to the email address: casework@ico.org.uk

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Matters reported to the ICO should also require a separate report to the Charity Commission, but this should be carefully checked as to where the data protection duty lies because Serious Incident reports are subject to Freedom of Information requests which may, if answered, create a further data or privacy breach if the lines of responsibility are not clear.

Individuals should be notified when a data breach is *"likely to result in a high risk to the rights and freedoms of natural persons… without undue delay.*" When notifying individuals, where the likely harm is high risk whether from embarrassment or loss of privacy, or exposure to fraud, specific and clear advice should be given on what they can do to protect themselves and what the School is able to do to help them. The School should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to mitigate the risks posed by the breach.

**Review and Evaluation**

Once the initial aftermath of the breach is over, the Head should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Full Directors' meetings for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. It should be considered whether the breach warrants a disciplinary investigation. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

**Implementation**

The Head should ensure that staff are aware of the School's data protection policies and their requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's data protection policies and their requirements, they should discuss this with the Head.

**Data breaches caused, or suffered, by suppliers**

By law suppliers must notify the School "*without undue delay*" if they become aware first. Wychwood, Oxford then has an obligation to report begins once we are first made aware.

Appendix A - **Wychwood Office, Administration and Archive Filing**

## 1. Girls' Files in Main Office

**Spine Label** of Orange file gives name as in Ann ANOTHER
followed by date which marks Trinity Shell Form year.
[If not in school at this point e.g. Study entry or short term visitor, date in brackets.]

**Coloured dots:**
= Study only (known at start of course)
= short term visitor (known in advance)
= here for GCSE } coloured dots can only be affixed when girl has left.
= left early }

This dating system and coloured dots are in use for Old Girls' records and have been for past 30-40 years.

**Green Manilla Wallet cover:**

**ANN ANOTHER** **Shell year** **Date of Birth**
[brackets if known not to be here in Shell]

ENTRY: term, date and form on entry
LEFT: term, date and form on leaving

**Plastic wallets**

- in this order, with yellow on top.
- all filed chronologically, with most recent on top. List below gives order of groups within wallets.

**Yellow: GENERAL:** absence notes; prep absence/presence; general ephemeral correspondence
boarding permissions, travel, general ephemeral correspondence with parents/guardians
uniform, major ps if not challenged; routine letters re dates, occasions, events etc.
general correspondence which does not have longer term responses or history needed.

**Red: ACADEMIC; interview and conversation records post entry**
replies to academic forms e.g. choices at GCSE, AS and A**2**
Letters from parents and notes of any conversations re. academic issues. (Any communication re problems with staff/teaching should be in a sealed A5 envelope with label with name and "Confidential, Academic".
Copies of letters and reports about scholarships at Remove or Study level.
Copies of references for other schools, or rough notes if no formal record.

Copies of UCAS references and rough notes from subject teachers.

**Green:** **PASTORAL**: All correspondence and records of phone calls with bearing on pastoral care.
Confidential material sealed and with label “Confidential, Pastoral”.
SEND: IEPs, Statements, Ed Psych reports: all filed and kept as per the Data Requesting. Storage, Retention and Disposal policy
Records of extra time and other Access requirements for public examinations.

**Blue: FINANCIAL**: all matters financial including reminders, bank transfers, bursaries etc.
Sensitive information to be sealed in an envelope as above, “Confidential, Financial”.

**Clear: ENTRANCE** : **ACCEPTANCE FORM** with all the crucial data
Correspondence with parents post offer
Scholarship and Bursary details if relevant
Written Entrance papers
Initial correspondence with parents/guardians.