Data Protection Policy

This policy applies to all activities undertaken by The Girls' Education Company Limited, Registered Charity No. 310638, trading as Wycombe Abbey, and its subsidiary companies, including Wycombe Abbey Services Limited (Company No. 2510811), Wycombe Abbey Developments Limited (Company No. 09547970), Wycombe Abbey International Limited (Company No. 09911805), and Wycombe Abbey Pension Trustees Limited (Company No. 3743179) (referred to in this policy as "we", "us" or "our").

This policy is intended to support compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Privacy and Electronic Communications Regulations 2003 (PECR), and the Data (Use and Access) Act 2025 (DUAA). The Information Commissioner's Office (ICO) is responsible for enforcing data protection law.

Our ICO registration numbers are:
Girls' Education Company Limited – Z5311880;
Wycombe Abbey Services Limited - ZB014569; and
Wycombe Abbey Foundation – ZC124088.

Data protection is an important compliance issue. In the course of our activities, personal data (sometimes sensitive in nature) is collected, stored and processed. As a data controller, we are responsible for how personal data is handled. Everyone therefore has a role to play in ensuring that we comply with our legal obligations, whether the data handling is sensitive or routine.

Executive Summary for all staff and contractors:

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- *Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?*
- *Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?*
- *What would be the consequences of my losing or misdirecting this personal data?*

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how to handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

1. Application of this Policy

This policy applies to staff (past, present and prospective), including employees, workers, volunteers, apprentices and Council members (collectively referred to as "**staff**" for the purposes of this Policy).

Staff should refer to the associated privacy notices and, where appropriate, to other relevant policies including in relation to the use of internet, email and communications, social media, AI tools, data retention and acceptable use of IT policy, which contain further information regarding the protection of personal information in those contexts.

All staff who handle personal data are obliged to comply with this policy and must read and understand this policy because it gives important information about:

- the data protection principles with which we must comply;
- data protection obligations;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how data is gathered, used and (ultimately) deleted, whether personal information or sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information gathered used, stored or transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Contractors – This policy sets the standard of compliance expected of contractors who handle personal data, whether they act as data processors on our behalf (and are therefore subject to contractual terms) or as independent data controllers in their own right. Where we share personal data with a third party – for example other schools, universities, parents, authorities or professional advisers – each party must have an appropriate lawful basis and handle the data lawfully, securely and confidentially.

2. Introduction

We obtain, keep and use personal information (also referred to as data) about job applicants and current and former employees, workers, contractors, volunteers, Council members and apprentices for a number of specific lawful purposes, as set out in our *Staff Privacy Notice*.

We also obtain, keep and use personal information about prospective students, current pupils, their families, Seniors, Friends of Wycombe Abbey and residents at the School. Details of how this information is collected and processed are set out in the separate *Privacy Notice for Parents and Pupils, Privacy Notice for Seniors and Friends of Wycombe Abbey, and Privacy Notice for Residents*.

This policy sets out how we comply with data protection obligations and seek to protect personal information relating to stakeholders. Its purpose is also to ensure that everyone understands and complies with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

Anyone who handles personal data must comply with this policy. Breaches may lead to disciplinary action being considered. We recognise that accidental breaches or near misses can happen through human error and will not always amount to misconduct; however, failures to report incidents or near misses that create a significant risk to the School or to individuals will be treated seriously.

The Bursar has overall responsibility for Data Protection as a member of the Executive Leadership Team. We have appointed the Head of Compliance to act as data privacy lead undertaking staff training around data protection and privacy compliance. The Head of Compliance is responsible for monitoring compliance with data protection obligations and with our policies.

3. Definitions

The following definitions shall apply to this policy:

"**data controller**" means the person or body that determines the purposes and means of the processing of personal data, and who is legally responsible for how the data is used. For example, we are a data controller. An independent contractor who makes their own such decisions is also, separately likely to be a data controller.

"**data processor**" means the person or organisation that processes (handles) the data on behalf of the data controller. For example, a payroll software provider with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

"data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

"data subject" means the individual to whom the personal information relates;

"personal information" (sometimes known as personal data) means information relating to a living individual who can be identified (directly or indirectly) from that information, it can include any form of identifier, digital or contextual, including unique ID numbers, initials, nicknames. This definition includes expressions of opinion or intentions towards that individual. Note that personal information will be created almost constantly in the ordinary course of work duties (such as emails, notes of calls, management information records, minutes of meetings);

"processing" means virtually anything done with personal information including obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

"pseudonymised" means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

"sensitive personal information" (sometimes known as '**special categories of personal data'** or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation; and

"criminal records information" means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures. There are separate rules for the processing of personal data relating to criminal convictions and offences.

4. Data Protection Principles

GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- processed **lawfully, fairly** and in a **transparent** manner;
- collected for **specific and explicit purposes** and only for the purposes it was collected;
- **relevant** and **limited** to what is necessary for the purposes it is processed;
- **accurate** and kept **up to date**;
- **kept no longer than is necessary** for the purposes for which it is processed; and
- processed in a manner that ensures **appropriate security** of personal data.

The GDPR's broader accountability principle also requires us not only to process personal data lawfully, fairly and transparently, but also to be able to demonstrate that we do so. This includes, among other things:

- keeping records of all data processing activities, including by way of logs (using the online application) and policies;

- documenting significant decisions and assessments about how personal data is used (including via formal risk assessment documents called Data Protection Impact Assessments - DPIA); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

5. Lawful grounds for processing personal information

Each processing activity must have a lawful basis. The School must not only process personal data fairly and lawfully, but also be able to demonstrate that the processing is lawful.

Before any processing starts, and while it continues, the following requirements must be met:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing;
- except where the processing is based on consent, satisfy that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document decisions as to which lawful basis applies, to help demonstrate compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see '**Sensitive Personal Information**' section below), and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

Staff must discuss any new processing activity, project or system change with the Head of Compliance before work begins. This ensures that data protection requirements are considered early and that any necessary assessments can be completed in time.

6. Sensitive Personal Information

We may from time to time need to process sensitive personal information. Sensitive personal information will only be processed if:

- there is a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with our legal obligations or for the purposes of our legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g:
    - the data subject has given explicit consent;
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the School or the data subject;
    - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
    - processing relates to personal data which is manifestly made public by the data subject;
    - the processing is necessary for the establishment, exercise or defence of legal claims; or
    - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must be satisfied that the criteria above are met and must document their decision. Where sensitive personal information will be processed for the first time, staff must notify the Head of Compliance in advance so that an appropriate assessment can be completed before the data is collected or used.

Our privacy notices set out the types of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

7. Processing Safeguarding Information

We will ensure that staff understand the relevant data protection principles which allow the sharing (and withholding) of personal information including:

- being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal and should be treated as 'special category personal data'
- understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows the sharing of special category personal data, including without consent where there is good reason to do so. For example, information may be shared without consent where: it is not possible to gain consent; it cannot be reasonably expected to gain consent; and gaining consent would place a child at risk
- not providing pupils' personal data where the serious harm test is met.

Staff should refer to the *Safeguarding and Child Protection Policy* for further information.

8. Processing of Financial Information and Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Staff who are unsure in this regard must seek further guidance from the Director of Finance. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

9. Criminal Records Information

Criminal records information will be processed in accordance with our *Safer Recruitment policy*.

10. Using Third Party platforms / suppliers - Data Protection Impact Assessments (DPIA)

Before processing begins, a due diligence DPIA must be carried out to:

- to evaluate whether the processing is necessary and proportionate in relation to its purpose;
- assess the risks to individuals;
- identify any sort of artificial intelligence (AI) technology; and
- what measures can be put in place to address those risks and protect personal information.

Before any new service or system is purchased, the responsible manager must contact the Head of Compliance so that a DPIA can be completed if required. This process can take time, so early engagement is important.

Staff should also consider wider safeguarding issues linked to new technology and the Age Appropriate Design Code. In some cases, a separate assessment will be needed to decide whether the system requires approval from Digital Compliance Team before purchase. Click here for the New Software Application/Website/Ed Tech assessment form.

We keep written records of processing activities, and we review the personal information processed and update documentation accordingly.

11. Documentation and Record-Keeping

It is important that personal data held by us is accurate, fair and adequate. Staff are required to record their own data, and that of others, in a way that is professional and appropriate.

All staff should be aware that individuals have rights over personal data held about them in business records, including emails, notes, WHR and CPOMS/iSAMS records. This should not prevent staff from making necessary and accurate records of incidents or conversations involving colleagues, pupils or parents. In some cases there may be lawful grounds to withhold information, but staff should always record information in a professional way they would be prepared to justify if later disclosed.

12. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have specific legal rights. The most significant is the right of access to personal data held by the School, usually referred to as a subject access request. A request does not need to be in writing or use legal terminology. If you become aware of a subject access request, or any communication from an individual about their personal data, you must tell the Bursar or Head of Compliance as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- complain to us about a data protection issue (e.g. if they are unhappy with the response to their subject access request or how we have collected or used their personal information);
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.
- contest or seek human intervention in cases of solely automated individual decision-making, (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

These rights are not absolute and are often subject to legal exemptions, so each request must be assessed carefully before the School responds.

If you receive a request from an individual seeking to exercise one or more of their data protection rights, or raising a data protection complaint, you must tell the Bursar or Head of Compliance as soon as possible. Statutory response times apply, so prompt escalation is essential.

13. Data Security: online and digital

Some staff will have access to the personal information of staff, pupils, parents, suppliers, contractors and Council members in the course of their work. Where this applies, staff must ensure that their data protection obligations to those individuals are met.

Where staff have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not staff to access personal information if they have specific authority to do so from their line manager;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions) as well as using AI applications set out in our *AI Policy and Acceptable Use of IT Policy*;
- not remove personal information, or devices containing personal information (or which can be used to access it), from our premises unless appropriate security measures are in place (such as encryption and password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices.

Staff should contact the Data Breach Team (the Bursar, Head of IT Services and Head of Compliance) – via this link, which is also available in the staff handbook, if they are concerned that any of the following has happened, may have happened, or is likely to happen:

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions set out above under the heading '**Sensitive Personal Information**' being met;
- any data breach as set out under the heading '**Data Breaches**' below;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from our premises without appropriate security measures being in place; or
- any other breach of this Policy or of any of the data protection principles set out under the heading '**Data Protection Principles**' above.

14. Information Security

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

These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where we use external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions from us;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent from us and under a written contract;
- the organisation will assist in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist in meeting our GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to us as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide us with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell us immediately if it is asked to do something infringing data protection law.

Before entering into any new agreement involving the processing of personal information by an external organisation, or changing an existing agreement or process, the relevant line manager must seek guidance from the Digital Compliance Team. A DPIA will also usually be required.

In summary, the *Acceptable Use of IT Policy* includes:

- Staff are responsible for the security of the data they have. Measures need to be in place to ensure the security of the data. Acceptable measures include the use of encrypted devices.
- Use of personal email accounts or unencrypted personal devices by staff for official business is not permitted.
- The sharing of information should be done using secure systems. See Appendix 1 for further details.

15. Storage and Retention of Personal Information

Personal information (and sensitive personal information) will be kept securely in accordance with the *Data Management and Retention Policy* and relevant privacy notices.

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Data Retention Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Head of Compliance.

Limited personal data is retained for archiving purposes where it is necessary to do so in the public interest, for scientific or historical research purposes or statistical purposes subject to appropriate safeguards being put in place to protect the rights and freedoms of the data subject.

16. Data Breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure (including power outage);
- human error, such as accidental deletion or alteration of data;

- accidentally sending information to the wrong email address;
- unforeseen circumstances, such as a fire or flood;
- inputting personal or sensitive data into an AI application;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the person who holds it.

If staff become aware of, or suspect, a data breach, they must not investigate it themselves. They must report it to the Data Breach Team immediately, and in any event as soon as possible within 24 hours, while preserving any relevant evidence. See Appendix 2 for how breaches are handled.

17. International Transfers

The School may transfer personal information outside the UK on the basis that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses, compliance with this approved code of conduct and the completion of a risk assessment with suitable control measures via a DPIA.

18. Training

We will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or receive subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

19. Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for both us and the individual; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with it may lead to disciplinary action under the School's procedures and, in serious cases, dismissal for gross misconduct. If a non-employee breaches this policy, their contract may be terminated with immediate effect.

If staff have any questions or concerns about anything in this policy, they should contact the Head of Compliance.

20. Data Governance

The School has an IT Strategy Group (ITSG) which has Data Protection as a standing item on the agenda. Data Breaches which are notified to the ICO are also reported to the Council's Risk Committee.

Member of staff	Bursar / Head of Compliance
Reviewed	August 2026

Version: STDP/v14/26

Related Policies

Privacy Notices - For Staff, Parents, Pupils, Residents, Seniors and Friends, Summer Programme

Safer Recruitment Policy
Online Safety Policy
Social Media Policy
Acceptable Use of IT Policy (For Staff, Volunteers and Council Members)
Staff Code of Conduct
Data Management and Retention Policy
CCTV Policy
Taking, Using and Storing Images of Pupils Policy
Whistleblowing Policy
Safeguarding and Child Protection Policy – Sharing of Information
AI – Staff guidance in use of Artificial Intelligence

Appendix 1

Data Protection Guidance - Reminders on safely sharing information

Email:

Sending to "all staff " put in BCC line (not the To or CC field)

To **avoid** including **personal data** in emails, where possible

To start a **new email** conversation, where possible

To avoid the **Reply All** option

To carefully check that you have the correct recipient. Easy visual checks … staff have (WA Staff) displayed in their name, in the outlook directory staff names start with first name and include a job title. Pupils emails start with a number and on display you will see their house name.

Include a link to OneDrive, SharePoint or Teams wherever possible rather than an attachment. If an attachment is necessary and it includes personal data, password-protect the document.

Email groups:

To be checked by Head of Department at the beginning of each term or when new people start. Contact IT Helpdesk to correct for you.

Teams/SharePoint Files and Folders:

The Head of Department / Team Owner to check the Team Members at the beginning of each term and update accordingly. (Teams involving teaching groups is automatically updated via iSAMS)

The default setting for sharing from these areas is "**People with existing access"** these are for people who will already have access provided as part of the team or teaching group, or people you have previously shared with.

Sharing with a wider group requires staff to specifically select a different option - at "**Specific People" and adding in their name.**

It is possible to select from the dropdown menu **People in Wycombe Abbey or Anyone in your organisation.** However, please note that by selecting these option gives the recipient the ability to share/distribute to both staff and pupils, including being forwarded on within the organisation. It cannot be shared externally.

SharePoint Sites:

The default setting will be **Site owners, members and people with edit permission can share files and folders but only site owners can share the entire site.**

The "Allow access" request ***to be switched on for site owners*** *to allow access when a recipient requests permission.*

Requesting access for specific people. This enables you to send to others but you then have to authorise their access, this provides a useful recheck. It also means that the receiving person cannot forward onto anyone else. Only the site owner can do that.

One Drive:

There are a number of options to share a document.
The default setting is "**Specific People".** You can change this yourself but you should be aware of the implications:
People in the Organisation with the link – Only select when the document does not contain personal or commercial information. This link can be spread amongst Pupils and Staff

People with existing access – this option is for when the document has already been shared with people or groups. This link cannot be forwarded to other people.

Specific People – This is the safest option but you do need to ensure you select the correct person. Care needs to be taken.

You might also wish to select **block download or restrict editing** .

You can also decide whether recipients can **edit or view**.

Share and Copy Link both have the same settings as above. Use **copy link** when you are adding to the content of an email to multiple people or inserting to a SharePoint page such as MyWycombe or the Staff Handbook.

This option should not be available to select.

Anyone with the link – only select when the document does not contain personal or commercial information. *This link can be spread far and* wide, including externally.

Appendix 2

Handling a Data Breach

The Data Breach Team – Head of Compliance, Bursar and Head of IT Services will take the following steps:

Containment and recovery

The Data Breach Team will lead on investigating the breach.
It will be established:

- who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This may include isolating or closing a compromised section of the network, finding a lost piece of equipment and/or changing the access codes;
- whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up hardware to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts;
- which authorities, if relevant, need to be informed.

Assessment of ongoing risk

The following points will be considered in assessing the ongoing risk of the data breach:

- what type of data is involved?
- how sensitive is it?
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- regardless of what has happened to the data, what could the data tell a third party about the individual?
- how many individuals' personal data are affected by the breach?
- who are the individuals whose data has been breached?
- what harm can come to those individuals?
- are there wider consequences to consider such as a loss of public confidence in an important service we provide?

Notification of breach

Notification will take place to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Evaluation and response

Once a data breach has been resolved, a full investigation of the incident will take place. This will include:

- reviewing what data is held and where and how it is stored
- identifying where risks and weak points in security measures lie (for example, use of portable storage devices or access to public networks)
- reviewing methods of data sharing and transmission
- increasing staff awareness of data security and filling gaps through training or tailored advice
- reviewing contingency plans

The School will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.