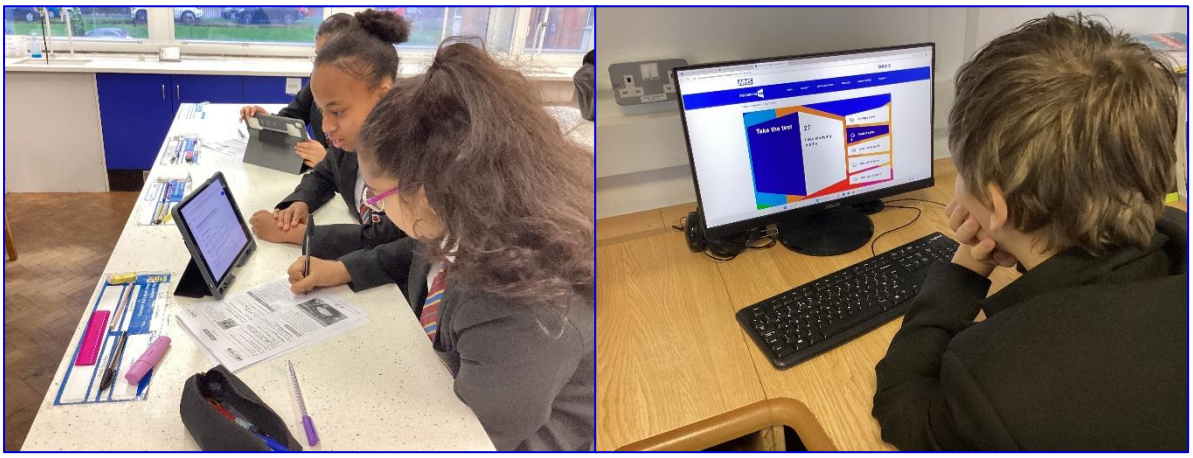

Data Protection Policy

School Workforce

"... I guarded them and not one of them perished..., so that the Scripture would be fulfilled."

John 17:12

Data Protection Policy: School Workforce

Contents

IMPORTANT: Please refer to the School Management Guide for important information about using this document.

Data Protection Policy of Saint John Wall Catholic School ("the School")

It is essential that you read and understand this Policy.

1. Introduction

1.1 This Policy sets out the principles that the School will follow in relation to personal data that it holds about all data subjects including yourself and others. It also sets out your obligations as a member of the workforce in relation to personal data. This Policy applies to the School's entire workforce including employees, consultants, contractors, temporary staff, full time and part time workers, volunteers and interns/work experience workers.

1.2 If you have any questions about this Policy, for example, whether information amounts to personal data and / or whether certain actions amount to processing you should contact the Headteacher.

1.3 Data protection laws protect personal data about identifiable individuals both in their private and professional capacities. As an organisation, the School may have personal data about employees, contractors, pupils, parents and carers, contacts and others. This Policy relates to the obligations of the School's workforce in relation to the personal data of any data subject that is processed by the School and its workforce.

1.4 You should be aware that failure to comply with your responsibilities under this Policy may amount to misconduct and that certain breaches of data protection laws can lead to personal criminal liability for you and to liability for the School. At the very least it may damage our reputation or affect our ability to use personal data which would have serious consequences for our organisation.

2. Definitions

For the purposes of understanding this Policy, the following definitions have the following meanings:

2.1 "Data Controller" means a person or organisation that processes personal data about a living individual. The School is a data controller for personal data we process about you. Other organisations such as the HMRC or your pension provider will also be data controllers.

2.2 "Personal Data" means data relating to or about an identifiable living individual. We process personal data about you as our employee. We also process personal data relating to our pupils, their relatives and carers and others.

2.3 "Special Category Personal Data" is a category of personal data which includes information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation. We may process some sensitive personal data about you as our employee. In the course of the provision of educational services and compliance with our statutory obligations we may also process sensitive personal data relating to our pupils and others.

2.4 "Data Subject" means an individual who is the subject of personal data. This includes job applicants, employees, consultants, agency workers, temporary staff, casual workers, contract workers, work-experience placements, gap-year students and ex-employees, pupils and their parents or carers and others with whom we have contact.

2.5 "Processing" includes the holding, obtaining, recording, organising, retrieving, consulting, using, adapting, altering, disclosing, transferring, disseminating and destroying of information. Processing extends to any operation or set of operations carried out on information or data and therefore covers everything we do with personal data.

2.6 "Communications Facilities" means, but is not limited to, telephones (mobile and desk), internet, intranet, email, applications, application data, supporting infrastructure and fax.

2.7 "Computer" means any device that can access the School's information such as a smartphone, laptop, tablet, or similar network-enabled device.

2.8 "Information Systems" means the School's Computers and its Communications Facilities.

3. Processing data

3.1 The School processes personal data (both manually and electronically), including sensitive personal data, for a number of reasons, including but not limited to:

- recruitment, appraisals, promotions, career planning, training and the provision of references;
- payment of salary and benefits, payroll, taxation, national insurance (and other statutory or contractual deductions from salary), reimbursement of expenses and business travel;
- health and safety matters;
- review and management of HR policies and procedures;
- disciplinary, grievance and performance management;
- and other purposes required by law, regulation or as deemed necessary by the School for the management of its employees and its business.
- information relating to children and others such as parents and carers relating to education and care, including pastoral care, assessment, development, progress, attendance, contact details, characteristics such as ethnic group, special educational needs and medical information.

3.2 Sensitive personal data relating to the workforce is only processed by the School for monitoring equal opportunities, diversity and staff welfare and for the purpose of providing specific services to individuals, including but not limited to:

- sickness absence, sick pay, suitability and fitness for work, health and safety control or as a result of medical or psychological examinations conducted at the School's request;
- maternity, paternity, adoption leave and pay, parental leave and / or time off for family and dependants;
- the School's obligations under the Equality Act 2010;
- absence control; and
- as required or permitted by applicable laws and regulations.

4. Collection of data

4.1 The School collects and records personal data from various sources, including by obtaining information from data subjects themselves.

4.2 In some circumstances, data may be collected indirectly from monitoring devices (including but not limited to door access-control mechanisms, closed-circuit television and other security systems, telephone, e-mail and internet-access logs and recordings).

4.2.1 Save for data collected from the School's security systems, data collected indirectly from monitoring devices is not routinely accessed but access is possible. Such data may be processed in circumstances including but not limited to the investigation of security breaches, abuse of the School's

Information Systems, or where the data is required for regulatory or law enforcement purposes.

5. Disclosure and Transfers

5.1 From time to time the School may transfer personal data (including sensitive personal data) outside the United Kingdom for the purposes set out above. We will ensure that appropriate safeguards are in place for personal data. Such restricted transfers will only be made where the UK has issued adequacy regulations covering the destination, or where an appropriate safeguard (such as the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses) is in place.

5.2 Personal data may also be transferred to third parties to process only on the School's instructions subject to confidentiality arrangements approved by the School.

5.3 We may need to share personal data with external organisations such as pension providers, healthcare scheme providers, trade unions, the local authority, professional and regulatory bodies and other similar service providers. We may disclose personal data in order to comply with a legal or regulatory obligation.

5.4 We will pass your personal data to Occupational Health who will hold information about your medical health and may share this with your managers and others in the organisation. This will be explained to you more fully at the time.

5.5 The School is subject to the Freedom of Information Act 2000 and this means that some information about you may be subject to disclosure to others in accordance with our statutory duties under that Act. Certain exemptions do exist which allow us to refuse access to information that we hold, for example, where information is protected by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. However, we are still legally required to consider each request for disclosure of information on an individual basis. Further information on the School's Freedom of Information Policy is available from the Headteacher.

6. Retaining Data – see Information Management Toolkit for School on https://irms.org.uk/page/SchoolsToolkit

6.1 The School endeavours to ensure that the personal data held is accurate and that inaccurate, irrelevant and excessive information is either deleted or rendered anonymous as soon as reasonably practical. However, the School may retain some personal data (including sensitive personal data) in order to comply with legal and regulatory obligations and for other legitimate business and or organisational reasons.

6.2 The School reserves the right, at its absolute discretion, to retain personal data (including sensitive personal data) after the termination of your employment, for purposes including but not limited to equal opportunities monitoring, health and safety records, to comply with statutory and regulatory requirements and in relation to possible or actual legal claims.

7. Security

7.1 The School must take appropriate technical and organisational security measures to protect personal data and to prevent any unauthorised or unlawful processing or its loss, damage or destruction. Factors involved when considering whether security measures are appropriate include the nature of the personal data and the potential harm which could result from unauthorised access.

7.2 If you are in possession of personal data (including but not limited to data held in spreadsheets, contained in CVs, contact lists or address books) you are obliged to

ensure that such personal data is kept in a safe place and is not accessed by unauthorised persons. You should use secure filing cabinets and password protected computer applications as appropriate.

7.3 If you become aware of any incident (actual or suspected) relating to security of data (including but not limited to personal data) you must immediately notify the **Data Protection Officer.** Examples of a security related incident can be incidents which may affect business continuity within the School or have a direct impact on the Confidentiality, Integrity or Availability of Information assets. Examples of these include: an unauthorised access of the premises or systems such as by a burglar; unauthorised access of personal data by a member of staff; loss of availability of the system or equipment; back up failure; theft of equipment; virus outbreak/threat; system downtime; loss of power; breach of confidentiality of data or breach of legislation. The Data Protection Officers are Mr Mariusz Wieremiewicz and Miss Kelly Chohan. The Data Protection Officer email is dpo@sjw.bham.sch.uk.

7.4 Computer equipment should always be safeguarded against unauthorised access, especially when left unattended. When working at School, you are required to screenlock your computer prior to leaving it unattended. Log out of your workstation when you leave your workstation for any length of time and switch off your workstation at the end of each working day.

7.5 When working on School related business away from the School's premises (working remotely), you must:

7.5.1 position yourself so that your work cannot be overlooked;

7.5.2 take reasonable precautions to safeguard the security of your Computer and any equipment on which you do the School's business, and keep any passwords secret;

7.5.3 as far as is reasonably practicable, keep with you at all times any Computer or other equipment on which you do School's work when not in use. Where this is not practicable, such equipment should be safely secured and kept out of sight of others. Such equipment should never be left unattended in public places. It should not be left in sight in cars, public transport or public buildings such as hotels. They should not be kept on desks overnight but stored in locked cupboards/drawers or taken home. They must not be left in vehicles overnight. When travelling you must always carry them in hand luggage.

7.5.4 inform the Police and the IT Department as soon as is reasonably practicable if either a laptop in your possession or any equipment on which you do the School work or store data relating to School work has been lost or stolen. (You will need a police crime number and report);

7.5.5 ensure that any work that you do remotely is saved onto the School's systems or is transferred to the School's systems as soon as is reasonably practicable.

7.5.6 ensure that memory sticks are kept separately from Computer equipment when not in use and are password protected memory sticks.

7.5.7 ensure that any data stored on your personal computer or other personal equipment is authorised. You should take appropriate steps (technical and otherwise) to ensure that School data held on personal computers or other personal equipment is protected from unauthorised and or unlawful access or use, accidental loss or destruction and theft.

7.6 You are required to undertake the following physical security steps to protect data:

7.6.1 Copying any information from School Systems onto any external media is prohibited unless justified for legitimate school purposes. Where the use of external media (such as memory sticks) is unavoidable, the data transferred must be encrypted and must be the minimum necessary for business purposes.

7.6.2 No sensitive, proprietary or confidential information is to be stored on unapproved peripheral devices or portable media (e.g. external USB drives, personal smartphones, or memory cards) outside the School systems.

7.6.3 No peripheral devices may be plugged into, installed or configured on any of the School's Computers.

7.7 You are required to comply with the following obligations in respect of portable media:

7.7.1 Portable media (e.g. data sticks, CDs, DVDs etc.) should only be used to transport or store data when other more secure means are not available and only when authorised by the IT department. All portable devices used to transport or store data should be encrypted in accordance with the School's encryption Policy.

7.7.2 All media should be stored in a safe place and manner in line with manufacturer's recommendations. Media safes, with appropriate fire resistance, should be used for business critical or sensitive data.

7.7.3 Care must be taken when transferring data from outside the School onto the School's Information Systems. All data must be swept for malicious software prior to the transfer.

7.7.4 Any loss or theft of any item of removable media must be immediately reported to the IT Department.

7.7.5 Where passwords have been shared or disclosed, you must change the password.

7.7.6 You must install and keep up-to-date a virus checker and firewall on your home-based computer if you transfer data between work and home. The School will not reimburse any part of the cost of home-based computer security, nor will it be responsible for any problem or virus that may be found on personal hardware.

7.8 Compliance with this Clause 7 is in addition to compliance with any other relevant School Policy relating to the use of Computers and related equipment or laws.

8. Your rights

8.1 You have the right to request access to personal data held about you. To exercise this right, contact the Data Protection Officer at dpo@sjw.bham.sch.uk. No fee will be charged unless the request is manifestly unfounded or excessive.

8.2 You have the right to object to use of your personal data for marketing purposes. If you wish to exercise this right at any time you should contact the Headteacher

8.3 In addition to the right of access, you also have the right (in certain circumstances) to rectification of inaccurate data, erasure, restriction of processing, data portability, and to object to processing, as well as rights in relation to automated decision-making. You also have the right to lodge a complaint with the Information Commissioner's Office (www.ico.org.uk) if you are unhappy with how the School has handled your personal data.

9. Monitoring of Communications by the School

9.1 You must use the School's Information Systems sensibly, professionally, lawfully, consistently with your duties, with respect for your colleagues and pupils and in accordance with this Policy and other relevant policies and rules. You must not use, or knowingly allow others to use these facilities to cause any nuisance or annoyance or inconvenience to any person or organisation.

9.2 A certain amount of responsible personal use of the School's Information Systems is permitted: nevertheless this Policy applies equally to such personal use. Particular

care should be taken when using the internet and email. Please see below for more details.

9.3 Internet access is provided at our discretion and will be monitored by us in accordance with this section.

9.4 The School is ultimately responsible for all organisational communications but subject to that will, so far as is possible and appropriate, respect your privacy and autonomy whilst working. The School may monitor your work communications for reasons which include: providing evidence of business and organisational transactions, ensuring that School procedures, policies and contracts with staff are adhered to; to ensure compliance with any legal obligations; for monitoring standards of service; staff performance and for staff training; preventing or detecting unauthorised use of our communications systems or criminal activities; and for maintaining the effective operation of our communication systems.

9.5 We will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject, date and time of text messages; non-business attachments to email; numbers called and duration of calls; domain names of web sites visited, duration of visits; and non-business files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes outlined above. You need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you visit web sites which detail the activities of a particular political party or religious group, then these visits might indicate your political opinions or religious beliefs. **By carrying out such activities using our Communications Facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.**

9.6 Any emails which are not stored in your "Personal" folder in your mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications since we have no way of knowing that they were intended to be personal. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this Policy. In particular, you are responsible to anybody outside the school who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy which may be caused by your failure to file your personal email. Ask the IT department how to do this.

9.7 In certain circumstances we may, subject to compliance with local laws and regulations, access email marked PERSONAL and access the content of what you have looked at or downloaded from the internet including, but not limited to, personal email sites such as Yahoo and Hotmail. An example of when we might do this is when we have reasonable suspicion that they may reveal evidence of unlawful activity such as where there may be a breach of contract with the School or Local Authority.

9.8 You must not use the internet to access any inappropriate, sexually explicit or unlawful material. Anyone deliberately or knowingly accessing such material may face criminal prosecution as well as internal disciplinary action which could include dismissal. Examples of inappropriate websites are those relating to pornography, illegal drugs, criminal activities, gambling and some forms of online merchandising but this list is not exhaustive. Should you inadvertently or accidentally access such a site you should immediately exit it and inform the IT Department as soon as practicable.

10. Data Breach

Under the UK GDPR, where a personal data breach is likely to result in a risk to individuals, the School must report it to the Information Commissioner's Office (ICO) without undue delay

and, where feasible, within 72 hours of becoming aware of it. Where the breach is likely to result in a high risk to individuals, those affected must also be informed without undue delay. Every actual or suspected breach must be reported internally to the Data Protection Officer immediately (see clause 7.3) so that this assessment can be made and any deadline met.
A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish 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 could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do 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 tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police.

Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- 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 relate; 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? 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
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- 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.

Notification of breaches

Informing people and organisations that you have experienced a data security breach can be an important element in your breach management strategy.

However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is 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.

From 26 May 2011 certain organisations (service providers) have a requirement to notify the Commissioner, and in some cases individuals themselves, of personal data security breaches. For more information about the specific breach notification requirements for service providers see:

https://ico.org.uk/for-organisations/guide-to-pecr/security-of-services

Answering the following questions will assist other types of organisations in deciding whether to notify:

- Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances, in other areas sector specific rules may lead you towards issuing a notification.

- Can notification help you meet your security obligations with regard to the security principle under the UK GDPR (Article 5(1)(f))?

- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?

- If a large number of people are affected, or there are very serious consequences, you should inform the ICO.

- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.

You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:

- Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data

- 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

- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already 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 you are willing to do to help them

- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform us if the media are aware of the breach so that we can manage any increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.

The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from us on receipt of their notification. This guidance is available at:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience. You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.
The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and nontechnical staff who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- If your organisation already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches
- It is recommended that at the very least you identify a group of people responsible for reacting to reported breaches of security

Other considerations

Additional guidance is also available if you need further information on data security breaches:

- See Notification of data security breaches to the Information Commissioner's Office.

More information

- This guidance will be reviewed and considered from time to time in line with new decisions of the Information Commissioner, Tribunals and courts.
- It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.
- If you need any more information about this or any other aspect of freedom of information or data protection, please Contact us: see our website www.ico.org.uk.

11. Your Additional Responsibilities

11.1 In addition to your obligations under this Policy, you must notify the Headteacher immediately of any changes in your personal circumstances, which could cause the information held to become inaccurate.

11.2 Should circumstances arise which could lead to a data breach (ie: theft, loss of items) you must immediately email dpo@sjw.bham.sch.uk and contact a senior member of staff by telephone.

Ratified by Governors: 24/06/2026
Review Date: 24/06/2027
(This policy will remain in force beyond the review date if no updates are required)