Data protection and information governance policy

Policy statement

The Whitgift Foundation, known as John Whitgift Foundation (the "Foundation") is committed to being transparent about how it collects and uses the personal data of its governors, staff, pupils, parents, residents, and clients to meet its data protection obligations. This policy sets out the Foundation's commitment to data protection and how it collects, uses, stores, and protects personal data, and the rights of individuals whose data we process.

This policy applies to the personal data of governors, job applicants, employees, workers, contractors, volunteers, apprentices, and former employees, referred to as HR-related personal data; and encompasses all personal data processed by the Foundation, in any format (electronic, paper, or otherwise). This policy also applies to the personal data of pupils, parents, residents, relatives and clients of the Foundation's care services.

The Foundation is the *Data Controller* for the purposes of data protection law. This means that the Foundation determines the purposes for which, and the manner in which, personal data is processed. The Chief Executive Officer is the Foundation's Data Protection Lead and is responsible for monitoring compliance, advising on obligations and acting as a contact point for the ICO. Any questions about this policy, or requests for further information, should be directed to the Chief Executive Officer at John Whitgift Foundation, North End, Croydon, CR9 1SS or via email (roishahughes@johnwhitgiftfoundation.org).

Legislation

This policy has been written in accordance with the UK General Data Protection Regulations and the Data Protection Act 2018.

Definitions

Personal data is any information that relates to a living individual who can be identified from that information, either directly or indirectly.

Processing is any use that is made of data, including collecting, storing, using, amending, disclosing, or destroying it.

Special categories of personal data refer to information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data and biometric data.

Criminal records data means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data subject is the individual to whom the personal data relates.

1. Data protection principles

The Foundation processes personal data in accordance with the following data protection principles. The Foundation:

a) Processes personal data lawfully, fairly and in a transparent manner.

b) Collects personal data only for specified, explicit and legitimate purposes.

c) Processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.

d) Keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

e) Keeps personal data only for the period necessary for processing.

Adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

The Foundation will only process personal data where there is a lawful basis for doing so. This may include:

- Consent
- Performance of a contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

The lawful basis relied upon will be documented for each processing activity.

Special category data will only be processed where:

- A valid Article 9 condition (specified under the UK GDPR) exists
- Appropriate safeguards are in place
- Processing is strictly necessary.

Additional security and confidentiality measures will apply to such data.

The Foundation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the Foundation processes special categories of personal data, such as ethnicity data, the information is given on a voluntary basis and will only be used for anonymised monitoring purposes. The Foundation also processes other personal sensitive data, such as medical information, in order to maintain the health and wellbeing of pupils and residents.

The Foundation is required by law to undertake criminal records checks for governors and those who are working with children or vulnerable adults. The information gathered will only be used for the purpose of determining suitability for the relevant role.

The Foundation will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered is held in the individual's personal file in hard copy and in electronic format on various IT systems. The periods for which the Foundation holds personal data are contained in the retention schedule attached to this policy as appendix 1.

2. Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

2.1 Subject access requests

Individuals have the right to access their personal data so that they are aware of and can verify the lawfulness of the processing. An individual is entitled to:

- confirmation that their data is being processed
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The Foundation will also provide the individual with a copy of their personal data that is being processed. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise.

To make a subject access request, the individual should send the request to:

Roisha Hughes
Chief Executive Officer
John Whitgift Foundation
North End
Croydon, CR9 1SS

E: roishahughes@johnwhitgiftfoundation.org

In some cases, it may be necessary to ask for proof of identification before the request can be processed; in such cases individuals will be informed and notified of the documents required to verify their identity. **If a subject access request is sent to a Foundation establishment, the Data Controller must be informed straight away so that it can be processed appropriately and within agreed timescales.**

The Foundation will normally respond to a subject access request within a period of one month from the date it is received. In some cases, such as where the request is complex or numerous, the timescale may be extended by a further two months. If this

is the case, the individual will be informed within one month of the receipt of the request of the extended timescale and why the extension is necessary.

Where the individual has requested a large quantity of data, the Foundation may ask the individual to specify the information the request relates to.

If a subject access request is manifestly unfounded or excessive, the Foundation is not obliged to comply with it. Alternatively, the Foundation can agree to respond but will charge a fee based on the administrative cost of responding to the request. For example, a subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Foundation has already responded. If an individual submits a request that is unfounded or excessive, the Foundation will notify them that this is the case and whether or not it will respond to it.

2.2 Other individual rights

Individuals have a number of other rights in relation to their personal data:

- to be informed
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object
- in relation to automated decision making and profiling

They (individuals) can require the Foundation to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the Foundation's legitimate grounds for processing data (where the Foundation relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Foundation's legitimate grounds for processing data.

To ask the Foundation to take any of these steps, the individual should send the request to Roisha Hughes at **roishahughes@johnwhitgiftfoundation.org**.

3. Data security

The Foundation takes the security of personal data very seriously. The Foundation has internal policies and controls in place to protect personal data against loss, accidental

destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. These include:

- Access controls and authentication (including multifactor authentication)
- Encryption, if appropriate
- Secure storage and disposal
- Regular data protection training
- Policies and procedures that are annually reviewed, as a minimum

The individual should refer to specific IT security policies at the establishment they are located at for more detail.

Where the Foundation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

The primary third-party organisations who process personal data on the Foundation's behalf are:

Atlas
Citation
Avantus
Baines Cutler
BUPA
Care Check
Care Quality Commission
Civica
Department for Education
HaysMac LLP
HMRC
Independent School Inspectorate
iHASCO
iSAMS
Management System
Medwyn Occupational Health
National Apprenticeship Service
NatWest
Networx
NHS
Person Centred Software
Planday
Sable International
Secondsight
Standard Life
TPS Pension Scheme
Travers Smith LLP
UKVI Sponsorship

4. Impact assessments

Some of the processing that the Foundation carries out may result in risks to privacy. Where processing would result in a high risk to an individual's rights and freedoms, the Foundation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

5. Data breaches

A data breach occurs when personal data (any data relating to an identified or identifiable natural living person) is destroyed, lost, altered or if there is unauthorised disclosure of (or access to) personal data as a result of a breach of security. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- 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.

Any breach of personal data, however small, must be reported to the Data Protection Lead as soon as possible after the breach has taken place (see appendix 3 - personal data breach reporting form).

Each breach of data will be assessed by the Data Protection Lead. If it is determined that the data breach poses a risk to the rights and freedoms of individuals, the Data Protection Lead will report it to the Information Commissioner within 72-hours of discovery.

The Foundation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Foundation will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

6. International data transfers

The Foundation may transfer some personal data outside the UK where necessary for operational purposes (for example, in relation to educational trips, service provision or use of specialist systems).

Where personal data is transferred internationally, the Foundation will ensure that appropriate safeguards are in place in accordance with UK data protection law. These may include:

- Transfers to countries that have been deemed by the UK Government to provide an adequate level of data protection;
- The use of approved contractual mechanisms, such as the UK International Data Transfer Agreement (IDTA) or other recognised safeguards; or
- Other lawful transfer mechanisms permitted under data protection legislation.

The Foundation will ensure that any such transfers are subject to appropriate risk assessment and that individuals' rights and freedoms are adequately protected. Further information about international transfers will be provided in relevant privacy notices.

7. Individual responsibilities

The Foundation may periodically ask individuals to check the personal information held on them so that they can ensure it is up to date. Individuals are responsible for keeping their personal data up to date and should let the Foundation know if any data they have provided changes, for example if an individual moves to a new house or changes their bank details.

Individuals may have access to the personal data of governors, employees, pupils, parents, or residents in the course of their employment or contract period. Where this is the case, the Foundation expects individuals to help meet its data protection obligations to staff, customers and clients and keep any personal data confidential and secure.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether inside or outside the Foundation) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- Not to remove personal data, or devices containing or that can be used to access personal data, from the Foundation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes.
- Report any breach of personal data, however small, to the Data Controller.

Further details about the Foundation's security procedures can be found in individual establishment's ICT usage policies.

In particular, an individual should ensure that they:

- use password-protected or encrypted software where available for the transmission and receipt of documents containing personal data
- lock files containing personal data in secure cabinets.

Where information is disposed of, individuals should ensure that it is destroyed securely. This may involve the permanent removal of the information from the server so that it does not remain in an individual's inbox or deleted folder. Hard copies of

information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an individual acquires any personal information in error by whatever means, they should inform the head of establishment or the Foundation's data controller immediately and, if it is not necessary for them to retain that information, arrange for it to be handled by the appropriate individual within the Foundation.

An individual must not take any personal information away from the Foundation's premises unless they have obtained the prior consent of the head of establishment or the Foundation's data controller.

If an individual is in any doubt about what their may or may not do with personal information, they should seek advice from the Foundation's data controller. If they cannot get in touch with the data controller, they should not disclose the information concerned until they have been able to do so.

8. Taking records containing personal data off site

An individual may only take certain records containing personal data off site where there is a valid reason given by the head of establishment or the Foundation's data controller.

Any individual taking records off site must ensure that they do not leave their laptop, other device or any hard copies of records in a public place such as on the train or in the car. They must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

9. Archiving and the destruction or erasure of records

All staff will receive basic training in data protection and management. Staff with specific responsibility for the management of records should ensure that:

- Records are stored securely, including where possible, with encryption so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable.
- Important records and large or sensitive personal databases are not taken home or carried or kept on portable devices (whether CDs, data sticks, mobiles, or handheld electronic tablets) unless absolutely necessary, in which case it will be subject to a risk assessment and authorisation by the head of establishment or the Foundation's data controller.
- Data back-up or migration is approached in line with the establishment's policy.
- Arrangements with external storage providers, whether physical, electronic or cloud based are supported by robust contractual arrangements providing for security and access.

- Reviews are conducted on a regular basis, to ensure that all information being kept is still relevant and, in the case of personal data, necessary for the purposes for which it is held, accurate and up to date.
- All destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use, disclosure or re-construction of any records or information contained in them.

Records are disposed of in line with the attached retention schedule – see appendix 1.

In many cases the prompt for review will be the end of a calendar year or tax year, so for the purpose of this policy a contingency is built in (e.g., seven years where the statutory limitation is six years).

Historic cases nationally, in the field of child protection, require a cautious approach to record retention, even the lifetime of a pupil. The school will ensure any long-term records are kept securely, accessible only by trained staff.

Insurance documents are not personal data and relevant historic policies are kept for as long as a claim might arise.

10. Secure disposal of documents

Confidential, sensitive, or personal information is considered securely disposed of when in a condition where the data cannot either be read or reconstructed.

Paper records are shredded or disposed of via a confidential waste disposal service; CDs, DVDs and diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

11. Child protection and document retention

In the light of cases of historical abuse, and the Independent Inquiry into Child Sexual Abuse which concluded in 2022, all schools are aware of the emphasis placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting.

The very proper focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are in suspension and Foundation schools are aware that they must not retain personal data longer or in greater volume than is necessary for its purpose, and that they must keep the data accurately or safely. The Foundation and Foundation schools will comply with a safeguarding requirement, first before applying normal retention periods to data, however sensitive.

12. Consequences of non-compliance

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Foundation's disciplinary procedures. Significant or deliberate breaches of this policy, such as accessing employee or pupil data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice, or pay in lieu of notice.

13. Monitoring

The Foundation may monitor employees, residents and pupils by various means including, but not limited to, recording individuals' activities on CCTV, checking emails and social media accounts, listening to voicemails and monitoring telephone conversations. If this is the case, the Foundation will inform the individual that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The individual will usually be entitled to be given a copy of any data that has been collected about them. The Foundation will not retain such data for any longer than is absolutely necessary.

In exceptional circumstances, the Foundation may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the Foundation by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means; for example, where an employee is suspected of stealing property belonging to the Foundation. Covert monitoring will take place only with the approval of the Foundation's data controller.

14. Training

The Foundation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

15. Right to complain

We are committed to protecting your personal data and handling it in a fair, transparent, and secure way. If you believe we have not handled your personal information in accordance with data protection laws, you have the right to make a complaint.

You can raise your concerns directly with us by contacting:

Roisha Hughes Email: roishahughes@johnwhitgiftfoundation.org
John Whitgift Foundation
North End
Croydon CR9 1SS

We will acknowledge your complaint promptly, investigate it thoroughly, and respond within one month.

If you are not satisfied with our response, or you prefer to raise the matter externally, you can contact the Information Commissioner's Office (ICO):

www.ico.org.uk Tel: 0303 123 1113

16. Policy dissemination and review

All employees should be made aware of this policy and its content in order that they are aware of their and the Foundation's responsibilities to keep all personal data secure in compliance with the data protection legislation. The policy will be accessible to all employees via Staff Zone and a hard copy can be accessed from the Foundation's HR department.

Employees should also make themselves aware of any supplementary data protection policy at the particular establishment that they are working at which should be read in conjunction with the Foundation's policy.

The policy will be reviewed at regular intervals and will be amended in line with any changes in the legislation that affect the Foundation or its employees' responsibilities.

The Governance Committee will be responsible for periodically reviewing compliance with this policy.

Ratification of policy

Name of policy:	Data Protection & Information Governance Policy
Policy created by:	Jane Fairall, HR Business Partner
Date policy reviewed:	August 2026
Policy approved by:	Governance Committee
Policy review date:	1 September 2028

Retention of records schedule

Type of record/document	Retention period
Foundation specific records	
Charity documents of Foundation	Permanent
Minutes, notes and resolutions of Court meetings	Permanent
Annual reports	Permanent
School specific records	
Minutes of governors' meetings	Permanent
Attendance register	7 years from last date of entry
Individual pupil records (including nursery)	
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision)
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: – pupil reports – pupil performance records – pupil medical records	25 years from date of birth, subject to where there are safeguarding considerations. In these cases, any material which may be relevant to potential claims will be kept for the lifetime of the pupil.
Special educational needs records (*to be risk assessed* individually)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
Bursary records	
Application form and initial financial assessment information (Form A)	If bursary application unsuccessful, retained for up to 12 months. If application successful, retained for the duration of time pupil in school
Financial assessment - annual (Form B)	Retained for the duration of time pupil in school and for a period of up to 12 months after leaving
Safeguarding - schools	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates	6 months from decision on recruitment, unless DBS specifically consulted. Record of the check must be kept on SCR

Type of record/document	Retention period
Single Central Register (SCR)	Keep a permanent record of all mandatory checks that have been undertaken
Accident / incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Files to be reviewed as part of the health & safety adviser review.
Child protection files	If a referral has been made/social care has been involved or child has been subject of a multi-agency plan – indefinitely If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely)
Residents' records	
Resident personal file containing – personal details – medical details Next of kin details	7 years from ceasing to be a resident/ service user
Carers' Information Service/Carers Support Centre clients	
Details of carer and cared for	Indefinitely in order to comply with any statutory or regulatory requirements for sharing personal data e.g., safeguarding
Accounting records	
Accounting records	6 years from the end of the financial year in which the transaction took place
Tax returns	7 years
VAT returns	7 years
Budget and internal financial reports	7 years
Contracts and agreements	
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	13 years from completion of contractual obligation or term of agreement

Type of record/document	Retention period
Intellectual property rights	
Formal documents of title (trademark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g., trademarks); otherwise, expiry of right plus 7 years
Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years)
IP/IT agreements (including software licences and ancillary agreements, e.g., maintenance; storage; development; coexistence agreements; consents)	7 years from completion of contractual obligation concerned or term of agreement
Insurance records	
Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim
Correspondence related to claims/renewals/ notification re: insurance	7 years
Environmental and health records	
Maintenance logs	10 years from date of last entry
Accidents to children	25 years from birth (unless safeguarding incident)
Accident at staff and visitors including RIDDOR	See Appendix 2
Staff use of hazardous substances	7 years from end of date of use
Risk assessments (carried out in respect of above	7 years from completion of relevant project, incident, activity or event
Employee records	
Application form, interview notes and selection records for unsuccessful candidates	12 months from application unless the candidate has consented to details being kept for future vacancies (or role has been given to a sponsored migrant – see below)
Disclosure and Barring Service checks and disclosures of criminal records forms	Up to 6 months following recruitment process unless assessed as relevant to ongoing employment relationship

Type of record/document	Retention period
General HR records – e.g., recruitment information, contract, references, qualifications, correspondence, appraisals, disciplinary records, grievances, sickness records	While employment continues and 7 years after it ends Except where safeguarding issue, relevant information kept indefinitely
Payroll and wage records (including details of overtime, bonuses, expenses, and benefits)	While employment continues and 7 years after it ends
PAYE records	While employment continues and 7 years after it ends
Records in relation to hours worked and payments made to workers	While employment continues and 7 years after it ends
Working time records	While employment continues and 7 years after it ends.
Parental leave records	5 years from child's birth/adoption (18 years for a disabled child)
Maternity records	While employment continues and 7 years after it ends
Sickness records required for the purposes of SSP	While employment continues and 7 years after it ends
Any reportable accident, death or injury in connection with work	See Appendix 2
Immigration checks	Throughout employment and for 2 years after employment ends.
Documents relating to sponsored migrants (e.g., evidence of satisfying the resident labour market test (where applicable) and evidence of the migrant's qualifications)	Throughout employment or until a compliance officer has examined and approved them (whichever is longer)

General Data Protection Regulations and the retention of accident and accident investigation reports

Policy and guidance – March 2018

Introduction

Social Security and health & safety legislation requires employers to record accidents that occur whilst people are at work and to report certain accidents, diseases, and dangerous occurrences to the enforcing authorities, i.e., Health and Safety Executive or local authority, within a given timeframe. Documenting employee workplace accidents in an Accident Book (BI510) is a requirement of Social Security legislation and the reporting of certain accidents, diseases and dangerous occurrences to the relevant enforcing authority is a requirement of health & safety legislation, under The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR), using the HSE's form F2508.

Whilst there is no specific legal requirement to investigate accidents, there is a moral duty and there is operational and business sense in carrying out an investigation in order to establish why an accident or injury occurred in the first place and to put appropriate measures in place to prevent harm or loss from happening again. It is inevitable that accident reports and the outcome of subsequent investigations will contain some personal information that will fall within the scope of GDPR, and which will be held on file for future reference.

This document outlines what is expected of John Whitgift Foundation (the Foundation) offices, schools, and care home establishments in terms of retaining their accident reports and any investigation findings that may contain personal information.

Summary of current accident reporting policy and guidance

It is the policy of the Foundation for each establishment to record and retain information on accidents that occur to people on their individual sites. This includes incidents that involve employees, pupils/students, elderly residents, and visitors to the sites. Details of the Foundation's accident reporting procedures can be found in Section 3 Part 3 of the Foundation's Health and Safety Policy and Management System Manual.

Each establishment management team is responsible for reporting any accidents that fall within the scope of RIDDOR to the relevant enforcing authority, using the HSE's Form F2508. A copy of that report must be forwarded to the Foundation's health and safety adviser so that an investigation can take place.

The Foundation's health and safety adviser must also be alerted to accidents and incidents that might fall outside of the RIDDOR reporting criteria and which could have been serious or have had serious consequences.

Each establishment management team is responsible for ensuring that any accidents and injuries involving employees are recorded in the Accident Book (BI510), irrespective of whether the accident is also reported under the requirements of RIDDOR.

Each establishment management team is responsible for ensuring that suitable records are kept on accidents and injuries that may involve school pupils/students, care home residents or visitors, i.e., non-employees.

Each establishment management team is responsible for investigating any minor accidents that may occur on each site from time to time. The Foundation's health and safety adviser will only get involved where accidents are reported under RIDDOR legislation or where there is the potential for a more serious outcome.

The implications of GDPR and retention of documentation

The following table outlines the policy with regards to retaining personal information held in accident report forms and any associated investigation forms.

Data item	Retention or review period	Comment
John Whitgift Foundation schools		
RIDDOR reports (F2508) – employees	7 years following end of employment or closure of file	When an employee leaves the school before 7 years following an incident, the RIDDOR report and any associated documentation must be retained by the relevant establishment
RIDDOR reports (F2508) – pupils & students	After 25th birthday (i.e., 7 years after leaving school at 18 years)	When a pupil/student leaves the school at 18, or earlier, the RIDDOR report and any associated documentation must be retained by the relevant establishment
RIDDOR reports (F2508) – visitors	7 years following closure of file	
RIDDOR reports where there may be a latent health issue as a result of an incident	40 years after incident	For example – unintentional exposure to a substance that is known to take time to have an adverse effect on the individual
Accident Book (BI510) - employee entries	3 years following entry or 12 years if industrial injury	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident record – third party entries (e.g., pupils/students, visitors)	3 years following record entry or after 25th birthday if pupil	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident or incident investigation reports containing personal information	7 years following closure of file	Reviews or disposal of accident investigation reports should form part of the RIDDOR report and Accident Book reviews

Data item	Retention or review period	Comment
John Whitgift Foundation care homes		
RIDDOR reports (F2508) - employees	7 years following end of employment or closure of file	If an employee leaves the care home before 7 years following an incident, the RIDDOR report and any associated documentation must be retained by the relevant establishment
RIDDOR reports (F2508) – elderly residents	7 years following closure of file	If an elderly resident leaves the care home before 7 years following an incident, the RIDDOR report and any associated documentation must be retained by the relevant establishment
RIDDOR reports (F2508) – visitors	7 years following closure of file	
RIDDOR reports where there may be a latent health issue as a result of an incident	40 years after incident	For example – unintentional exposure to a substance that is known to take time to have an adverse effect on the individual
Accident Book (BI510) - employee entries	3 years following record entry or 12 years if industrial injury	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident record – Third party entries (e.g., pupils/students, visitors)	3 years following record entry	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident or incident investigation reports containing personal information	7 years following closure of file	Reviews or disposal of accident investigation reports should form part of the RIDDOR report and Accident Book reviews
Whitgift Foundation offices		
RIDDOR reports (F2508) - employees	7 years after leaving employment or following closure of file	If an employee leaves before 7 years following an incident, the RIDDOR report and any associated documentation must be retained by the relevant establishment
RIDDOR reports (F2508) – visitors	7 years following closure of file	

Data item	Retention or review period	Comment
RIDDOR reports where there may be a latent health issue as a result of an incident	40 years after incident	For example – unintentional exposure to a substance that is known to take time to have an adverse effect on the individual
Accident Book (BI510) - employee entries	3 years following record entry or 12 years if industrial injury	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident record – third party entries (e.g., pupils/students, visitors)	3 years following record entry	Unless the accident report forms part of a RIDDOR investigation report, and the entry needs to be kept for evidence purposes – refer above
Accident or incident investigation reports containing personal information	7 years following closure of file	Reviews or disposal of accident investigation reports should form part of the RIDDOR report and Accident Book reviews

Personal data breach reporting form

This form should be used to report any breach of personal data, however small, and sent to the Foundation as Data Controller via Roisha Hughes, as soon as possible after the data breach has occurred

Name:	Location:
Job title:	Department:

About the breach

Please describe the breach - what happened and how it happened:

When did the breach occur?	Date:	Time:
When did you discover the breach?	Date:	Time:
Who did you report it to and when?	Name:	Date:
Was the breach caused by a cyber incident?		Yes / No

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, e.g., name, contact details
- ☐ Identification data, e.g., usernames, passwords
- ☐ Economic and financial data, e.g., credit card numbers, bank details
- ☐ Official documents, e.g., driving licenses
- ☐ Location data

☐ Genetic or biometric data ☐ Criminal convictions, offences ☐ Not yet known ☐ Other (please give details below)	
How many of personal data records were concerned?	
How many data subjects could be affected?	
Categories of data subjects affected (tick all that apply) ☐ Employees ☐ Pupils – current or past ☐ Parents – current, prospective, or past ☐ Residents/vulnerable adults – current or prospective ☐ Relatives/family members of residents – current or prospective ☐ Contractors ☐ Not yet known ☐ Other (please give details below)	
Actions taken as result of the breach Please describe what actions have been taken to prevent such a breach happening again:	
Data protection training When did you last receive data protection training?	
Signature Signed:	Dated:
Line manager Signed:	Dated:

This form should be signed by the individual reporting the breach and their line manager and then sent to Roisha Hughes at roishahughes@johnwhitgiftfoundation.org as soon after the breach as possible

Section 2 – to be completed by the Data Controller

Cyber incidents only

Has the confidentiality, integrity and/or availability of your information systems been affected? If yes, please tick all that apply:

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability

Please describe the impact on the organisation

- ☐ High – you have lost the ability to provide all critical services to all users
- ☐ Medium – you the ability to provide a critical service to some users
- ☐ Low – there is no loss of efficiency, or low loss of efficiency, and you can still provide all critical services to users
- ☐ Not yet known

Recovery time

- ☐ Regular – you can predict your recovery time, with existing resources
- ☐ Supplemented – you can predict your recovery time with additional resources
- ☐ Extended – you cannot predict your recovery time, and need extra resources
- ☐ Not recoverable – recovery from the incident is not possible, e.g., backups cannot be restored
- ☐ Complete – recovery is complete
- ☐ Not yet known

Likely consequences of the breach

Please use the data breach scoring matrix attached to assess the impact of the data breach

Probability	**Impact**	**Score**

Details:

Actions as a result of the breach Describe the actions that have been taken, or are proposed to take, as a result of the breach. Include, where appropriate, actions taken to fix the problem, and to mitigate any adverse effects, e.g., confirmed data sent in error has been destroyed, updated passwords, planning information security training.
Have you notified the data subject(s) about the breach? Please give reasons for your decision:
Have you notified, or are you planning to notify other organisations about the breach, e.g., the police, other regulators, or supervisory authorities? If yes, please specify:
Have you reported the breach to the ICO? Please give reasons for your decision: *NB breaches should be reported to the ICO within 72 hours of occurrence*

ICO Helpline: 0303 123 1113 (operates 9am to 5pm Monday to Friday)

Data breach scoring matrix

Ease of identification	
Personal data protected using strong encryption or otherwise cannot be matched to a subject	0
Personal data in clear text but cannot be easily matched to a subject without additional information	1
Personal data in clear text and can be easily matched to a subject	2

Circumstances of breach	
Personal data: disclosed to known recipients, modified or not available but can be restored and there is no evidence of illegal processing	0
Personal data: disclosed to unknown recipients; modified or not available but cannot be restored and there is no evidence of illegal processing	1
Personal data: disclose, modified or not available as a result of malicious behaviour	2

Data processing context	
Basic score where breach involves simple data and controller is not aware of any aggravating factors	0
Basic score where breach involves behavioral or financial data and controller is not aware of any aggravating or mitigating factors	1
Basic score where breach involves sensitive data and controller is not aware of any mitigating factors	2

Priority scoring

Score	Risk	Consequences	Response
0 – 2	Low	Subject may encounter minor inconvenience which can be overcome without difficulty	May be handled in line with local business process
3 – 4	Medium	Subject may encounter major inconvenience, which can be overcome with few difficulties	• CEO to be notified • Subjects may be notified as appropriate
5 – 6	High	Subject may encounter severe consequences which may prove difficult to overcome	• CEO to be notified • ICO to be notified • Subjects shall be notified as appropriate