Wellbrook School: GDPR & Data Protection Policy

WELLBROOK
SCHOOL

Reviewed by:	**C. Howells**
Last Review Date:	March 2026
Approved by:	A Sharma
Next Review Date:	March 2027
Version Number:	V4.0

Policy Statement

At Wellbrook School, we strive to provide every child with the opportunity to unlock their potential. We honour and celebrate their individuality and tailor our instruction to their personal needs. Our goal is to nurture self-confidence and provide students with the support necessary to help them reach heights they didn't think were possible. We want parents to imagine the possibilities when they walk through our doors and be filled with hope as they see their children achieve beyond their expectations. We strive to be a place where children feel they belong and can thrive.

We are also committed to safeguarding our pupils and staff and this policy outlines one of the ways we do that – by protecting their personal privacy and upholding their individual rights.

Introduction

- Wellbrook School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).
- We may, from time to time, be required to share personal information about our staff or pupils with other organisations, such as placing local authorities, other schools and educational bodies, and potentially social care services and the police.
- This policy is in place to ensure all staff, the proprietor / directors are aware of their responsibilities and outlines how the organisation complies with the following core principles of the GDPR.
- This policy complies with the requirements set out in the GDPR, which was effective from 25 May 2018 onwards.

Personal Data

- Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.
- Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The GDPR applies to both automated personal data and to manual filing systems, where

personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key- coded.

- Sensitive personal data is referred to in the GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters.
- Wellbrook School collects personal data in relation to staff and pupil records. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of placing local authorities, government agencies and other bodies.

Legal Framework

- This policy has due regard to legislation, including, but not limited to the following:
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

Wellbrook School takes technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. There are transparent privacy arrangements, which follow. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Data Protection Officer (DPO) VS. Data Compliance Officer

Under the GDPR, a data controller will only be required to appoint a DPO if any of the below three conditions are met:

- The processing is carried out by a 'public authority'.
- The 'core activities' require regular and systematic monitoring of data subjects on a 'large scale'.
- Where 'core activities' involve 'large scale' processing of 'special categories' of personal data and relating to criminal convictions and offences.

In the case of Wellbrook School none of these conditions are met, as outlined below, and therefore the school is not required to appoint a DPO.

- As an independent school, Wellbrook School does not qualify as a 'public authority'. This is affirmed by the definitions of 'public authority' and 'public body' given in both the Freedom of Information Act 2000 and the Data Protection Act 2018.
- As an educational provision, the 'core activity' at Wellbrook School is teaching, supplemented by therapeutic support, which does not inherently entail regular and systematic monitoring of data subjects on a 'large scale'.
- Neither the number of data subjects monitored, nor the volume of personal data processed by Wellbrook School qualifies as 'large scale' by a reasonable interpretation of the term, which remains undefined in statute.

In contrast to the statutorily defined role and position of a DPO, Wellbrook School employs a more flexible and equitable approach. All members of the school's leadership team are effectively data protection 'champions' and are expected to promote and uphold best practice within the remit of their role and among the staff they oversee. For the purposes of centralising organisational responsibility, a data compliance officer has been designated. Ultimately, however, it remains the responsibility of the data controller (the school) to make final decisions about whether to report a breach, disclose or amend a record or agree the terms of a contract with a data processor; the data compliance officer's role is merely to offer advice and guidance.

Our Data Compliance Officer is Anita Sharma

Like a DPO, the data compliance officer will:

- monitor the organisation's compliance with the GDPR
- report to the highest level of management, which is the executive head
- not be subject to dismissal, discipline or penalty for performing their duties.

Lawful Processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person. Sensitive data will only be processed under the following conditions:
- Explicit consent of the data subject, unless reliance on consent is prohibited by law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject.
- Carrying out obligations under employment.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- Wellbrook School ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- The consent of parents is sought prior to the processing of a child's data, including therapeutic or counselling services offered directly to a child. The data produced in therapeutic services is confidential to therapist and client, with the exception of safeguarding concerns and supervision (legally required).

The Right to be Informed

- We provide a clear, concise, and accessible privacy notice to individuals regarding the processing of their personal data. This notice is written in plain language and supplied free of charge (see Appendices 1 and 2).
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual

requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

- Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.
- When personal data is collected directly from the data subject (e.g., when admitting a pupil or recruiting a member of staff), we will provide the relevant privacy information at the time of collection.
- When personal data is obtained from another source (e.g., from a previous school, local authority, or safeguarding organisation), we will provide the privacy information:
    - Within one month of receiving the data;
    - Before we disclose the data to another recipient, if this will happen sooner; or
    - At the latest, at the time of our first communication with the individual, if that occurs before one month has passed.

The Right of Access

- Individuals have the right to obtain confirmation that their data is being processed.
- Individuals have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- Wellbrook School will verify the identity of the person making the request before any information is supplied.
- A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.

- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, Wellbrook School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- In the event that a large quantity of information is being processed about an individual, we will ask the individual to specify the information the request is in relation to.

The Right to Rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible.
- Where appropriate, Wellbrook School will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, Wellbrook School will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Individuals have the right to erasure in the following circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Wellbrook School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- The exercise or defence of legal claims
- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

- Individuals have the right to block or suppress Wellbrook School' processing of personal data.
- In the event that processing is restricted, we will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

Wellbrook School will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data
- Where an individual has objected to the processing, and we are considering whether their legitimate grounds override those of the individual
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where we no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim
- If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

We will inform individuals when a restriction on processing has been lifted.

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means, personal data will be provided in a structured, commonly used and machine-readable form.

Wellbrook School will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Wellbrook School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

Wellbrook School will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Object

Wellbrook School will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

An individual's grounds for objecting must relate to his or her particular situation.

Wellbrook School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the organisation can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- Wellbrook School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- Wellbrook School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, we will offer a method for individuals to object online.

Privacy by Design and Privacy Impact Assessment

Wellbrook School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the organisation has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the organisation's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Wellbrook School' reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

Wellbrook School will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, we will consult the INFORMATION COMMISSION to seek its opinion as to whether the processing operation complies with the GDPR.

Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The leadership team will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Wellbrook School becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at Wellbrook School, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the data compliance officer
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach

- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Data Security

- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records are not left unattended or in clear view anywhere with general access.
- Where data is saved on removable storage or a portable device, the device is kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, Wellbrook School enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff are advised to not use their personal laptops or computers for work purposes.
- All necessary members of staff are provided with their own secure login and password. Any users with access to sensitive material held within Google Drive have two factor authentication enforced for their account, ensuring that even if their password is compromised the data to which they have access is still inaccessible to any would-be intruder.
- Documents attached to emails with sensitive or confidential information are password-protected.
- Wellbrook School only emails parents very occasionally, usually only in response to an email from a parent, if a parent has specifically requested to be emailed or if other means of communication have failed.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from the organisation's premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of Wellbrook School containing sensitive information are supervised at all times.

The physical security of the organisation's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Wellbrook School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action. The school ensures that continuity and recovery measures are in place to ensure the security of protected data.

Publication of Information

Wellbrook School makes only the following information routinely available:

- policies and procedures.

Wellbrook School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the schools' website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and Photography

Wellbrook School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

Wellbrook School notifies all pupils, staff and visitors of the purpose for collecting CCTV images. There is appropriate, clear signage at all sites.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose in our special school context.

All CCTV footage will be kept for security purposes; the duration for which depends on the school site. Please see the school's CCTV policy.

Wellbrook School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If Wellbrook School wishes to use images/video footage of pupils in a publication, such as the schools' website, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

Dashcams on School Vehicles

In addition to fixed CCTV cameras on the school site, Wellbrook School operates dashcams on its minibuses. These cameras capture video recordings of pupils, staff, and members of the public while vehicles are in use.

The lawful basis for this processing is the School's legitimate interests in safeguarding, promoting safety, protecting school property, and supporting investigations into incidents or accidents. Dashcam footage is handled in accordance with the same principles that apply to CCTV, including strict retention periods, secure storage, limited access, and individuals' rights under data protection law.

Data Retention

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted as soon as practicable.
- Some educational records relating to former pupils or employees of Wellbrook School may be kept for an extended period for legal reasons, but also to enable the provision of references.
- Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS Data

- All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Use of Secure Email Systems and Non-secure Email Systems

The majority of communication with local authorities and social care services is via secure email systems. Where this is not the case, all emails must reference children, colleagues and others related to the business of our schools, using initials only.

When using non-secure emails, content must be thought through before the 'send' button is pressed. If there is any potential concern regarding confidentiality or breaching data protection guidance, the email should not be sent.

All wellbrookschool.co.uk emails have a disclaimer hyperlink (see appendix 4).

Information Requests (See Appendix 3)

- Wellbrook School will respond within one calendar month from the date of receipt to any written or emailed request for information it holds or publishes unless an extension is applied. If the request is complex or involves multiple requests, the time limit can be extended by a further two months, but the Wellbrook School must the requester within the initial month about the extension and the reasons for it.
- The schools will provide information on where to access the information required e.g., the website link, or details of a charge if the publication/ information is charged or send any free information. If the item is charged the schools do not need to provide it until the payment is received
- A refusal of any information requested must state the relevant exemption which has been applied or that the schools do not hold the information, and must explain what public interest test has been made, if this applies
- If the information is published by another organisation (for example, Ofsted reports) the schools can direct the enquirer to the organisation which supplied the information or publication unless it is legal and possible to provide the information directly
- It will not be legal to photocopy a publication in its entirety and supply this to an enquirer unless the schools own the copyright – this is particularly important where the original publication was a charged item
- The schools will keep the original request and note against this who dealt with the request and when the information was provided

- Any complaint about the provision of information will be handled by the executive head. All complaints should be in writing and documented.
- All enquirers should be advised that they may complain to the Information Commissioner if they are unhappy with the way their request has been handled
- Under the Freedom of Information Act a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. These can be requested if sufficient information is provided to identify them

Confidentiality (also see Appendix 4)

- Employees are required to keep confidential about Wellbrook School' business and that of its pupils and families both during their employment and at any time after its termination. All information gained in the course of an employee's employment, remains confidential except in circumstances in which they are required to disclose information to the schools. Employees must not remove any documents or tangible items which belong to the schools, or which contain any confidential information from the schools' premises at any time without due cause. This includes the unauthorised use of any headed paper containing the schools' logo and/or contact details.
- Employees must return to the schools if requested and, after consultation, and in any event upon the termination of your employment, all documents and tangible items which belong to Wellbrook School or which contain or refer to any confidential information and which are in their possession or under their control.
- Employees must, if requested by any leader, and after consultation, delete all confidential information from any re-usable material and destroy all other documents and tangible items which contain or refer to any confidential information and which are in their possession or under their control.
- Employees are not permitted to disclose information reproducing the schools' passwords or security codes to unauthorised personnel during their employment or at any time after termination of employment. Keys and electronic fobs allocated by the schools must not be passed on or made available to unauthorised persons within or external to the schools.

- Employees who have access to the schools' accounts and financial transactions are not permitted to disclose this information without the authorisation of the executive head or director.
- See appendix 4 for the confidentiality statement from all employees' contracts.

Retention of School Records and Personnel Information

School Records:

1.1 Where a pupil is on roll with Wellbrook School at the conclusion of the final academic year offered (year 11), the school takes responsibility for the secure retention and storage of their records, including CP/safeguarding files.

1.2 Where a pupil comes off the Wellbrook School roll before the conclusion of year 11, their records (including CP/safeguarding files) will be forwarded securely to their new school.

2.1 If the conditions of clause 1.1 are met and the child was looked after, all records (including CP/safeguarding files) will be retained until the child's 75th birthday.

2.2 If the conditions of clause 1.1 are met and clause 2.1 does not apply, CP/safeguarding files containing documentation relating to a referral to social services or any other social services involvement will be kept until 35 years from date the pupil leaves the school.

2.3 If the conditions of clause 1.1 are met and clause 2.1 does not apply, a pupil's records will be retained by Wellbrook School for 10 years, or until the conclusion of the academic year in which the pupil's year group reach their 25th birthday.

Personnel Information:

3.1 Where there has been a CP/safeguarding allegation made against a member of staff, the school will retain their personnel records for 10 years or until the employee reaches retirement age, whichever is the longer.

3.2 Any records that could be called as evidence in legal proceedings e.g., records relating to child sexual abuse concerns/disclosures or allegations against staff, must be kept indefinitely.

3.3 If clause 3.1 and 3.2 do not apply, staff files will be retained for 6 years after the employee has left the employment of Wellbrook School.

All physical files that are retained in accordance with the conditions outlined above are held in secure storage facilities until the expiration of their retention period, at which point they are securely destroyed.

All digital files that are retained in accordance with the conditions outlined above are securely and permanently deleted upon the expiration of their retention period.

Cyber-security incidents

Any individual that discovers a cyber-security incident will report this immediately to the headteacher and the DPO.

When an incident is raised, the DPO will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Whether the incident needs to be reported to the relevant authorities, e.g. the INFORMATION COMMISSION or police

The school's DPO will take the lead in investigating the incident, with assistance from the IT team, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised. The DPO will oversee a full investigation. The cause of the incident, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access

- The headteacher will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure

- In the event of any external or internal breach, the DPO will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information

- The school will organise updated staff training following a breach

- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where the security risk is high, the DPO will establish what steps need to be taken to prevent further data loss, which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.

- Taking systems offline.

- Retrieving any lost, stolen or otherwise unaccounted for data.

- Restricting access to systems entirely or to a small group.

- Backing up all existing data and storing it in a safe location.

- Reviewing basic security, including:

- Changing passwords and login details on electronic equipment.

- Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

Schools are required to report personal data breaches to the INFORMATION COMMISSION if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does not need to be reported; however, the school will need to justify this decision and document the breach.

The DPO will notify the INFORMATION COMMISSION within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the INFORMATION COMMISSION when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

The school will report a personal data breach via the INFORMATION COMMISSION website. The school will also make use of the INFORMATION COMMISSION's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the DPO will notify those concerned directly of the breach without undue delay.

Where the school has been subject to online fraud, scams or extortion, the DPO will also report this using the Action Fraud website.

The DPO and ICT technician will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

Appendix 1: Privacy Notice For Pupils

The main reason that the school processes personal data is because it is necessary in order to comply with the schools' legal obligations and to enable it to perform tasks carried out in the public interest.

The school may also process personal data if at least one of the following applies:

- in order to protect the vital interests of an individual
- there is explicit consent
- to comply with the schools' legal obligations in the field of employment and social security and social protection law
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- for reasons of public interest in the area of public health
- for reasons of substantial public interest, based on law, which is proportionate in the circumstances, and which has provided measures to safeguard the fundamental rights and the interests of the data subject.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, address and contact details, carers' details)
- Characteristics (such as ethnicity, language, nationality, country of birth, religion)
- Attendance information (such as sessions attended, number of absences and absence reasons, behavioural information, details of any exclusion information)
- national curriculum assessment results, examination results,
- where pupils go after they leave us
- any special educational needs or disabilities as well as relevant medical information.

We collect and hold personal information relating to our pupils and those involved in their care. We may also receive information from previous schools, the local authority and/or the Department for Education (DfE).

We use this personal data to:

- support our pupils' learning
- support our pupils' welfare
- monitor and report on their progress
- provide appropriate pastoral care.
- assess the quality of our services.
- process any complaints.
- protect vulnerable individuals.
- the prevention and detection of crime.

We may pass data to:

- the local authority
- schools that a pupil attends after leaving Wellbrook School
- The Department for Education (DfE)
- The NHS
- third-party organisations, as allowed by law
- agencies that provide services on our behalf
- agencies with whom we have a duty to co-operate
- External agencies, e.g., social care services, the police.

Personal data will not be retained by the schools for longer than necessary in relation to the purposes for which they were collected.

Wellbrook School may take photographs or videos of pupils for official use, monitoring and for educational purposes. You will be made aware that this is happening and the context in which the photograph will be used.

Photographs may also be taken of those attending an event which may appear in the media. You will be made aware that this is happening and the context in which the photograph will be used.

You have the right to:

- be informed of data processing (which is covered by this Privacy Notice)
- access information (also known as a Data Subject Access Request)
- have inaccuracies corrected
- have information erased
- restrict processing
- data portability (this is unlikely to be relevant)
- intervention in respect of automated decision making (this is unlikely to be relevant)
- Withdraw consent (see below)
- Complain to the Information Commissioner's Office (see below)

To exercise any of these rights please contact the data compliance officer:

Withdrawal of consent

The lawful basis upon which the schools process personal data is that it is necessary in order to comply with the schools' legal obligations and to enable it to perform tasks carried out in the public interest.

Where the school processes personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Complaints to INFORMATION COMMISSION

If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting the data compliance officer.

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally, the INFORMATION COMMISSION cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Appendix 2: Privacy Notice for Staff

The main reason that the schools processes personal data is because it is necessary in order to comply with the schools' legal obligations and to enable it to perform tasks carried out in the public interest.

The schools may also process personal data if at least one of the following applies:

- in order to protect the vital interests of an individual
- there is explicit consent
- to comply with the schools' legal obligations in the field of employment and social security and social protection law
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- for reasons of public interest in the area of public health
- for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, based on law, or pursuant to contract with a health professional
- for reasons of substantial public interest, based on law, which is proportionate in the circumstances, and which has provided measures to safeguard the fundamental rights and the interests of the data subject.

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- performance (such as capability and disciplinary matters)

- qualifications and recruitment information (and, where relevant, subjects taught)
- information relevant to the annual independent schools' census and absence information.

We process personal data relating to those we employ to work at, or otherwise engage to work at our schools:

- for recruitment and employment purposes
- to enable the development of a comprehensive picture of the workforce and how it is deployed
- to inform the development of recruitment and retention policies
- to assist in the running of the schools
- to enable individuals to be paid.

The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling equality monitoring
- protecting vulnerable individuals
- the prevention and detection of crime.

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

We will not give information about you to anyone outside the schools without your consent unless the law allows us to.

We share this information with the Department for Education (DfE)*

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

*We share personal data with the Department for Education (DfE) on a statutory basis as part of our annual census submission.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools. For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

To contact the department: https://www.gov.uk/contact-dfe.

Personal data will not be retained by the School for longer than necessary in relation to the purposes for which they were collected.

You have the right to:

- be informed of data processing (which is covered by this Privacy Notice)
- access information (also known as a Data Subject Access Request)
- have inaccuracies corrected
- have information erased
- restrict processing
- data portability (this is unlikely to be relevant)
- intervention in respect of automated decision making (this is unlikely to be relevant)
- withdraw consent (see below)
- complain to the Information Commissioner's Office (See below)

To exercise any of these rights please contact the data compliance officer:

Withdrawal of consent

The lawful basis upon which the schools process personal data is that it is necessary in order to comply with the schools' legal obligations and to enable it to perform tasks carried out in the public interest.

Where the schools process personal data solely on the basis that you have consented to the processing, you will have the right to withdraw that consent.

Complaints to INFORMATION COMMISSION

If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting the data compliance officer.

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner for a decision. Generally, the INFORMATION COMMISSION cannot make a decision unless you have exhausted our internal review procedure. The Information Commissioner can be contacted at:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Appendix 3: Procedures for responding to Data Subject Access Requests (SARs)

Any individual has the right to make a request to access the personal information held about them or their children.

Actioning a Data Subject Access Request

1. Requests for information must be made in writing, which includes email and be addressed to the data compliance officer. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of, as examples:

- Passport
- Driving licence
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand and the nature of the request. The data compliance officer, or an appropriate leader, should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not

deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The schools may make a reasonable administration charge for the provision of information.

5. The response time for Data Subject Access Requests, once officially received, is one calendar month. However, should the school require more information from the requester, they may “stop the clock”. Once the required information is received, the response time continues.

6. All information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the schools with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Dealing with Data Subject Access Requests involving other people's information

Where an information request is made in relation to information held on a person other than yourself or your child, information will not be provided unless full written consent has been given by the person or persons whose information is being requested. However, even before requesting this written consent, advice will be sought from the Information Commissioner's Office (INFORMATION COMMISSION).

Responding to Data Subject Access Requests that may involve providing information relating to another individual (a 'third party individual')

Data Subject Access Requests might, in the case of an employee file request for example, contain information identifying managers or colleagues who have contributed to (or are discussed in) that file. This may lead to a conflict between the requesting employee's right of access and the third party's rights over their own personal information.

To decide whether to disclose information relating to a third-party individual, we follow INFORMATION COMMISSION guidance.

Whatever the decision, we will always keep a record of our course of action and the reasoning for it.

Appendix 4: Confidentiality statement in Wellbrook School employee contracts

You will be required not to make any statements, whether written or oral, to the media or the public during your employment under this contract, or for a period of three years after its termination, concerning matters which might, or which is calculated to or which in the knowledge of a reasonable person would, adversely affect the best interest of Wellbrook School Limited.

Without the prior written consent of Wellbrook School, you will not divulge or publish any confidential information relating to the operation, running or administration of the schools which may come to your knowledge during your employment.

You will handle personal data in compliance with the Data Protection Act 1998 and the Company's Data Protection Policy at all times

Disclaimer statement from hyperlink at end of all Wellbrook School emails

All Wellbrook School emails and attachments are private and intended solely for the use of the individual or entity to whom they are addressed. Unauthorised use (for example disclosure, storage or copying) is not permitted. If you are not the intended recipient, please destroy all copies and inform the sender by return email.

Wellbrook School reserves the right to monitor, record and retain any incoming and outgoing emails for security reasons and for monitoring internal compliance with our online safety and use of ICT policy. Email monitoring and/or blocking software may be used and email content may be read.

Any views or opinions expressed in this email are solely those of the author and do not necessarily represent those of Wellbrook School.

Wellbrook School checks all emails and attachments for known malware, however, you are advised that you open any attachments at your own risk.

Wellbrook School may be required to disclose this email (or any response to it) under the Freedom of Information Act 2000 unless the information in it is covered by one of the exemptions in the Act.

Wellbrook School is owned by Wellbrook Education Limited (14695495).

Our registered office and address for correspondence is West Midlands House, Gipsy Lane, Willenhall, Wolverhampton, West Midlands. WV13 2HA

Our independent school registration number with the Department for Education is 830/6063. Our URN is: 150920