# Data Protection Policy

School Name: The White Horse Federation

Version No:

Ratified date: 14th December 2023

Author: Lyn Rouse

Interim Review Date: April 2024

Owner: Helen Peace

Next Review Date: August 2024

Approved by: Board of Trustees

## Executive Summary

The Data Protection Policy sets out the principles and guidelines for safeguarding sensitive information and ensuring compliance with data protection laws and regulations. It encompasses measures for data collection, storage, processing, and sharing, as well as outlines the responsibilities of all WHF individuals in upholding data protection standards. The policy aims to mitigate the risks associated with data breaches and unauthorised access, thereby fostering trust with stakeholders and maintaining the integrity of the organisation's data management practices.

## Contents

## 1. Aims

The White Horse Federation and their employees aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors, and other individuals is collected, stored and processed in accordance with legal safeguards specified in the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ('UK GDPR') the Data Protection Act ('DPA') 2018 and other regulations together Data Protection Legislation.

This policy applies to all Personal Data, regardless of whether it is in paper or electronic format.

It is the responsibility of all members of The White Horse Federation to take reasonable care when handling, using or transferring Personal Data so it cannot be accessed by anyone who does not:

- Have permission to access that data, and/or
- Need to have access to that data

Data breaches can have serious effects on individuals, schools and the whole federation concerned. It can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the federation, school and the individuals involved. All transfer of data is subject to risk of loss or contamination.

## 2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner Office (ICO) on the UK GDPR. Information Commissioner's Office (ICO)

It meets the requirements of the Protection of Freedom Act 2012 when referring to our use of biometric data. Protection of Freedoms Act 2012 (legislation.gov.uk)

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)

In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

| Terminology | Definition |
|---|---|
| Personal Data | Any information relating to an identified, or identifiable, natural person/individual. This may include the individuals:<br>Name<br>Identification number<br>Location<br>Online identified, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |
| Special Categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing includes transferring personal data to third parties. Processing can be automated or manual. |
| Data Subject | The identified or identifiable living individual whose personal data is held or processed. For the purpose of this policy this includes pupils, staff, parents and |

| | |
|---|---|
| | other individuals. A data subject need not be a UK national or resident. |
| Data Controller | A person or organisation that determines the purposes and the means of processing of personal data. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes. |
| Data processor | A person or organisation, other than an employee of the data controller, who processes personal on behalf of the data controller. |
| Personal data breach | A breach of security Leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |
| Biometric data | Information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting. |
| Biometric recognition system | Is a system that operates automatically (electronically) and<br>- Obtains or records information about a person's physical or behavioural characteristics or features and<br>- Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system |

## 4. The Data Controller

The White Horse Federation processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a **Data Controller**.

The White Horse Federation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and Responsibilities

This policy applies to everyone, all staff employed by our federation, those who volunteer in any capacity including but not limited to Trustees, Local governors, Parent helpers and to external organisations or individuals working on our behalf.

Staff who do not comply with this policy may face disciplinary action. This policy does not form part of any employee's contract of employment and may be amended at any time.

### 5.1 Trustees & Governing board

The board of Trustees have overall responsibility for ensuring that The White Horse Federation complies with all relevant data protection legislations.

The school governing bodies are overall responsible for ensuring their school complies with all relevant data protection legislations.

### 5.2 Data Protection Officer

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring compliance with Data Protection Legislation and developing related policies and guidelines where applicable.

The Data Protection Officer will provide an annual report of their activities directly to Trustees.

Our DPO is Lyn Rouse and is contactable via email at DPO@twhf.org.uk

The DPO will monitor internal compliance, inform and advise on data protection obligations and provide advice on DPIAs.

The DPO will be easily accessible as a point of contact for employees and individuals.

### 5.3 IT Network Managers as Information Asset Owners

Each secondary school within the White Horse Federation has assigned an IT Network Manager as an Information Asset Owner. The IT Network Manager will aid the Senior Head of IT and Head of GDPR by ensuring:

- That information flows smoothly between the Senior Head of IT, DPO and school
- Be aware, monitor and check all data assets and processing activities within your school
- Complete OneTrust questionnaires when required
- Be involved with Subject Access Requests by running exchange files when requested
- Challenge security of IT systems and employees working practice
- Complete incident forms
- Complete new supplier/ provider / solution forms
- Identify risks for data protection and report these immediately to the DPO.

### 5.4 Data Processors

We contract with various organisations who provide services to the Trust or School, including:

- School meal providers
- Healthcare, social and welfare organisations
- Police forces and / or courts
- Business associates and professional advisers
- Suppliers and service providers
- Education and examining bodies
- Local and Central government
- Website provider

In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

**Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy and in line with data subjects rights.
- Ensuring their personal data is up to date on the HR system
- All staff will be aware to contact the DPO in the following circumstances:

  - With any questions about the operation of this policy, Data Protection Legislation, retaining personal data or keeping personal data secure.
  - If they have any concerns that this policy is not being followed.
  - If they are unsure whether they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach without undue delay
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

### 5.5 Flow of information

The flow of information between the WHF Senior Management Team, the DPO and Trustee's will be as follows:

- There will be a secure folder shared between CEO, COO and DPO for updates.
- The DPO will provide updates for the Trustees at Risk and Audit Meetings.
- The DPO will provide an annual update for the Trustees.

## 6. Data Protection Principles

The Data Protection Legislation is based on data protection principles that the White Horse Federation must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and in a way which is not incompatible with those purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under Data Protection Legislation.

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract such as an employment contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

We will normally only process special category personal data under the following legal grounds:

Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
Where the processing is necessary for the reasons of substantial public interest, for example the purposes of equality of opportunity and treatment.
Where the processing is necessary for health or social care purposes, for example to pupils with medical conditions or disabilities; and
Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

**Vital interests**
There may be circumstances where it is considered necessary to process personal data or special category personal data in order to project the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in a very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

**Consent**
Where none of the other bases for processing set out above apply then the school must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When pupils and or our workforce join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

If consent is required for any other processing of personal data of any data subject then the form of this consent must:

Inform the data subject of exactly what we intend to do with their personal data;
Require them to positively confirm that they consent – we cannot ask them to opt-out rather opt-in; and
Inform the data subject how they can withdraw their consent

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

### Primary Schools

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

### Secondary Schools

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by Data Protection Legislation or as soon as possible thereafter unless we have already provided this information such as at the time when a pupil joins us.

The IT Network Manager will liaise with the DPO Lead to ensure that where it is required an effective DPIA has been established. To ensure a robust approach the Procurement Manager will also be involved in the process via the DPO.

## 7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our workforce).

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary unless otherwise specifically permitted by the Data Protection Legislation.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the White Horse Federation data deletion guidelines that can be found in section 16.

## 8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, Online Solution Providers. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with the Data Protection Legislation
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We may share personal data that we hold about data subjects and without their consent with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency 'ESFA', Ofsted, Health authorities and professionals, the Local Authority, examination bodies, other schools and other organisations where we have a lawful basis for doing so.

The UK GDPR does not prevent us from sharing personal data with law enforcement authorities (known under GDPR as competent authorities) who are discharging their statutory law enforcement functions. The UK GDPR and the DPA 2018 allow for this type of data sharing where it is necessary and proportionate. If you want to share personal data with a law enforcement authority you will need a lawful basis under Article 6 and if you are sharing special category data you will need a lawful basis under Article 6 and 9. Staff are expected to liaise with the DPO before submitting data to law enforcement authorities as it may come under the banner of a Subject Access Request.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of Tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, if personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

We may also share personal data with marketing companies who will deliver specifically target information to staff, parents / carers or pupils. Consent will be obtained before any marketing related communications are sent and will be

reviewed every 2 years. The individuals have the right to withdraw consent which can be requested via the DPO@twhf.org.uk email address.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with the Data Protection Legislation.

1.1 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

1.2 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Staff are responsible for ensuring that the information they are processing is only shared with individuals on a need to know basis sharing facts when they need to know.

Staff should refrain from sharing sensitive information via email, a more secure method of sharing information is to share a folder between individuals. Later, when appropriate, the owner can remove sharing permissions to that folder.

## 9. Subject Access Requests and Other Rights of Individuals

A person has the right to know how their personal data is being processed, they also have the right to access that data, this is called a Subject Access Request ("SAR"). A person can make SAR verbally, in writing or by social media.

A SAR could include all or some of the following:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

It is helpful if the person submits their request online via our website: https://thewhitehorsefederation.org.uk/gdpr.

If staff receive a subject access request in any other format they must immediately forward it to the DPO immediately. We have a statutory obligation to complete the request within 1 Calendar month.

Please see appendix 3 for SAR Procedures.

### 9.1 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, aged 13 or over, the child must either be unable to understand their

rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school aged under 13 years may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## 9.2 Responding to Subject Access Requests

The DPO will respond and acknowledge all SAR requests. Our statutory obligation is to provide the information within 1 calendar month. This can be extended for up to two additional months due to the complexity of the request, the sensitivity nature of the request or if the personal data is mixed up with information about others whose privacy we must carefully consider. If it is deemed necessary to extend we will inform the individual immediately.

We would request that SARs are not made near or during the school holidays as lack of resources during these periods, it may be necessary for us to extend the period in which we can respond, this is due to pertinent staff being unavailable to retrieve information.

Exam results are confidential until after the published date and will not be included in any SAR request prior to this date.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 calendar month of receipt of the request
- Confirm the requesters address
- May ask for clarification, this could include; are there any specific types of information required? Which staff members do you think may hold the information? What are the date ranges for the information?

We will not disclose information if:

- By disclosing may cause serious harm to the physical or mental health of the pupil or another individual
- By disclosing would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- The information is contained in adoption or parental order records
- The information is given to a court in proceedings concerning a child
- The information is in relation to an open investigation.

We will usually deal with the request free of charge but if the request is considered to be manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be manifestly unfounded or excessive where there is no clear intention to access information or the request is otherwise malicious in intent.

This will be determined on the actions of the requester and content any of correspondence and can include but is not limited to:

- Repeated requests for the same information
- The Requester stating their intention is to cause disruption
- The request is making unsubstantiated accusations against the [Trust/Academy/School] or its staff
- Systematic or repeated requests are being made as part of a campaign with the intention of causing disruption

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

### 9.3 Other Data Protection Rights of The Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the school, online via the GDPR page or via email DPO@twhf.org.uk. If staff receive such a request, they must immediately forward it to the DPO.

If staff receive any type of request either verbally or written from an individual in respect of their personal data, please follow the procedure outlined in Appendix 3.

- Right to Be Informed: the individual is seeking information that should have been provided to them in the privacy notice, or the notice itself
- Right to Erasure: the individual is seeking that their data be deleted and/or 'forgotten'
- Right of Access: the individual is seeking confirmation that their data is being processed; access to, or a copy, their data, or other supplementary information

- Right to Rectification: the individual is claiming that their data is inaccurate or incomplete, and is seeking for it to be rectified
- Right to Data Portability: the individual is seeking a reusable copy of their data, or to have the data transmitted to another entity
- Right to withdraw consent: the individual is seeking to withdraw their consent to the processing of their data

### Freedom of Information Procedures

Freedom of Information requests or requests under the Environmental Information Regulations 2004 must be submitted in writing and we would request that this is done by emailing the DPO@twhf.org.uk.

The DPO will respond within 20 days of the original request. Staff on receiving a request for information under the Freedom of Information Act or Environmental Information Regulations must forward it to DPO@twhf.org.uk on the date on which it is received.

### Freedom of Information Policy

All schools are committed to comply with the relevant legislation pertaining to a Freedom of Information and/or Environmental Information Regulations request and will follow the guidance set out by the Information Commissioner's Office.

## 10. Parental requests to see their child's educational record

As we are an Academy we do not fall under the remit of the Education (Pupil Information) (England) Regulations, and parents will be required to adhere to this policy in making a Subject Access Request to view information on their child's educational records which is beyond that which is routinely provided to parents and carers.

## 11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get consent from at least one parent or carer before we take any biometric data from their child and first process it. This consent will be recorded within the individual school's Management Information System.

Parents/carers (of children under the age of 18) and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish or be provided with a payment card if applicable.

Parents/carers of children under the age of 18 and pupils can object to participation in the school's withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent/carer.

Where staff members or other adults use the school's biometric system(s) we will also obtain their consent before they first take part in it or at the commencement of their employment and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time and should do so in writing by emailing DPO@twhf.org.uk and the school will delete any relevant data already captured.

## 12. CCTV Details

We use CCTV across all federation establishments for the purpose of safeguarding (providing a safe and secure environment for pupils, staff and visitors) and security (to prevent the loss of or damage to the Trust buildings and assets and to assist in the prevention of crime and assist law enforcement agencies in apprehending offenders).

We use CCTV if we suspect pupil, staff and any third party conduct does not meet the White Horse Federation standards. If upon review a disciplinary action is observed, CCTV can be used for the purpose of a disciplinary investigation. CCTV will not be viewed solely for the purpose of monitoring behavior but will be subject for review if standards are thought to be breached. For the safety and well-being of individuals there are some areas that are continually monitored, these areas have additional signage.

We will adhere to the ICO's guidance for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

**Please see Appendix 4 for further CCTV information.**

Any enquiries about the CCTV system should be directed to Lyn Rouse DPO@twhf.org.uk

The DPO will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas;
- The CCTV system being encrypted/password protected;
- It is checked daily to ensure that it works sufficiently.
- Viewing is restricted, accessible only to those who have permission.
- Copies will only be made if absolutely necessary for safety or law enforcement purposes.
- Every effort will be made to ensure camera's do not record inappropriate images e.g. in a toilet cubicle.

Requests to view CCTV recordings by individuals will be considered as a **subject access request** and the footage will be viewed by an individual who has access and will view and send to the DPO for consideration on whether it can be shared.

If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual with access must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals then the Trust must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Trust.

## Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

## Primary Schools

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for school use, communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

## Secondary Schools

We will obtain written consent from parents/carers, or from pupils aged 13 and over, for photographs and videos to be taken of pupils for school use, communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

- Consent can be refused or withdrawn at any time.

If consent is withdrawn, we will delete the photograph or video and not distribute it further. To withdraw consent please complete the relevant form https://thewhitehorsefederation.org.uk/gdpr.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Where a child's image has been used in a prospectus or brochure which has been printed for the purposes of distribution, it may not be possible to remove the image of the child in all copies and this should be taken into account when providing any consent.

See our IT Video and Digital Image policy for more information on our use of photographs and videos.

## 13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant Data Protection Legislation (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO Lead will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on Data Protection Legislation, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of all our schools' IAO, The White Horse Federation DPO LEAD and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept in secure locations when not in use.

Papers containing confidential personal data must not be left unattended in offices, classrooms on staffroom tables, pinned to notice or display boards, or left anywhere else where there is general access.

- Where personal information needs to be taken off site, this will be agreed and recorded by the Head teacher.
- Staff passwords are used to access school computers and online resources, these must meet complexity rules which include the following rules:

  - 8 characters long

  - Containing letters, numbers and special characters

  - Must be changed every 90 days

  - The password cannot be the same as the last 10 previous passwords
- Failure to enter the correct password will lock the user's account. Please refer to the IT Password Policy for more information.
- As part of ongoing cyber security awareness for pupils, they're advised to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

  - Staff, pupils, governors,Trustees and third parties who store personal information must do so on WHF devices are expected to follow the same security procedures as staff and follow specific procedures such as 'GDPR Working Practices'
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data.

The White Horse Federation will follow the Impact Levels as follows:

| The White Horse Federation Marking Scheme | Impact Level (IL) | Release & Destruction Classification. |
|---|---|---|
| NOT PROTECTIVELY MARKED | 0 | None |
| CONFIDENTIAL | 1 | Securely shredded or securely deleted |
| HIGHLY CONFIDENTIAL | 2 | Securely shredded or securely deleted |

The schools will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer. Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students/pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "IL0, IL1 or IL2".

## Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the federation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection Legislation.

When an individual leaves employment of the White Horse Federation their emails will be deleted from the system 12 weeks after their departure date.

The following data retention periods apply for the categories below:

| **Employee and Ex-Employee Data** | | | |
|---|---|---|---|
| **Description / Record Type** | **Location of Stored Data** | **Retention / Disposal Period** | **Disposal Method** |
| Senior executives' records (that is, those on a senior management team or their equivalents) | HR Database & HR Cabinets | Permanently | Securely shredded or securely deleted / overwritten |
| Statutory Sick Pay records, calculations, certificates, self-certificates | HR Database & HR Cabinets | 6 years after the employment ceases | Securely shredded or securely deleted / overwritten |
| Ex-Employee Network Files and email | Shared drives and email | 12 weeks after leave date | Securely deleted |

| **Student Data** | | | |
|---|---|---|---|
| **Description** | **Location of** | **Retention / Disposal Period** | **Disposal Method** |
| Student Safeguarding Files | School Locked Cabinets | Data kept until individual 25 years old | Securely shredded |
| Ex Student Data (electronic) | School MIS - access controlled | Data kept until individual 25 years old | Securely deleted / overwritten |
| Ex Student Data (paper based) | School Locked Cabinets | Data kept until individual 25 years old | Securely shredded |

| Employee and Ex-Employee Data | | | |
|---|---|---|---|
| **Description / Record Type** | **Location of Stored Data** | **Retention / Disposal Period** | **Disposal Method** |
| Assessments under health and safety regulations and records of consultations with safety representatives and committees | HR Database & HR Cabinets | Permanently | Securely shredded or securely deleted / overwritten |
| Inland Revenue/HMRC approvals | HR Database & HR Cabinets | Permanently | Securely shredded or securely deleted / overwritten |
| Salary Sacrifice | HR Database & HR Cabinets | 6 years after employment ceases | Securely shredded or securely deleted / overwritten |
| Parental leave | HR Database & HR Cabinets | 18 years from the birth of the child | Securely shredded or securely deleted / overwritten |
| Pension records | HR Database & HR Cabinets | Until the employee reaches age 100. | Securely shredded or securely deleted / overwritten |
| Pension scheme investment policies | HR Database & HR Cabinets | 12 years from the ending of any benefit payable under the policy. | Securely shredded or securely deleted / overwritten |
| Terms and conditions | HR Database & HR Cabinets | review 6 years after employment ceases or the terms are superseded. | Securely shredded or securely deleted / overwritten |
| Termination of employment, for example early retirement, severance or death in service | HR Database & HR Cabinets | at least 6 years although the ICO's retention schedule suggests until employee reaches age 100. | Securely shredded or securely deleted / overwritten |
| Additional hours / sickness | HR Database & HR Cabinets | 6 years after the employment ceases | Securely shredded or securely deleted / overwritten |
| Trade union agreements | HR Database & HR Cabinets | 10 years after ceasing to be effective. | Securely shredded or securely deleted / overwritten |
| Personnel files and training records (including formal disciplinary records and working time records) | HR Database & HR Cabinets | 6 years after employment ceases | Securely shredded or securely deleted / overwritten |

| | | | |
|---|---|---|---|
| Recruitment application forms and interview notes (for unsuccessful candidates) | HR Database & HR Cabinets | 1 year | Securely shredded or securely deleted / overwritten |
| Redundancy details, calculations of payments, refunds, notification to the Secretary of State | HR Database & HR Cabinets | 6 years from the date of redundancy | Securely shredded or securely deleted / overwritten |

We will only keep data that is required by law, any other data will be deleted from the system within 3 months of the employee leaving.

Any requests for copies of work will be agreed by the CEO to ensure the business is not jeopardised in anyway by releasing this data.

## Personal Data Breaches

The White Horse Federation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised datase being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop or mobile device
- Misdirected email containing information about individuals that could identify directly or indirectly

## 1 Training

All staff and governors are provided with continued data protection training as part of their roles.

The COO and DPO will work together to ensure that all staff including contracted staff will receive annual GDPR training, this will also form part of individuals CPD.

This will be monitored by the DPO to ensure effectiveness across the Trust.

## 2 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every year and shared with all relevant stakeholders.

This policy will be reviewed when the Data Protection and Digital Information (No 2) Bill has been reported on.

## 3 Links with Other Policies

This data protection policy is linked to our:

Privacy Notice

- IT Video and Digital Image Policy
- Student Acceptable User Policy
- Staff Acceptable User Policy
- IT Password Policy
- IT Cloud Based Solution Policy

Appendix 1

## Personal Data Breach Procedure

The Trust is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

## Reporting Procedure

The breach must be reported **on the day of discovery** to the DPO Lyn Rouse by emailing DPO@twhf.org.uk or calling 07719 314166

- The DPO will determine whether the breach is reportable to the ICO, if necessary, the timeframe for reporting is 72hrs.

- The DPO will request for a form to be completed and returned to the DPO within a quick turnaround timeframe.

- The DPO will request to view the documentation that was breached.

- The DPO will identify trends in breaches across the organisation and identify possible training requirements.

This procedure is based on guidance on personal data breaches produced by the ICO.

On suspecting, finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO. A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

- Leaving a mobile device on a train;
- Theft of a bag containing paper documents.
- Destruction of the only copy of a document;
- Sending an email or attachment to the wrong recipient;
- Using an unauthorised email address to access personal data; or
- Leaving paper documents containing personal data in a place accessible to other people.

The DPO will advise on the best course of action.

- The DPO will consider whether personal data has been accidentally or unlawfully
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to be repeated.
- The DPO will work out whether the breach must be reported to the ICO or data subjects. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud resulting in financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding) -
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
    - Damage to reputation

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within the OneTrust platform.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data 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 personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will take appropriate action to ensure all individuals whose personal data has been breached are notified, usually. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored within the OneTrust platform.

The DPO and COO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

## Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- All staff to ensure they have a tidy desk and workspace.
- All staff to ensure that information is locked away.
- All staff to ensure their computer is password protected and to diligently lock their screen when away from their desk.
- All staff keep passwords confidential.
- All staff to complete GDPR / Data Protection training
- All staff to recognise when a breach has occurred and report accordingly
- All staff to recognise a SAR request and report accordingly

## Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it.
- There should not be any time delay between identifying a breach and taking steps to remedy the situation.
- In any cases where the recall is unsuccessful, the person who created the breach will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The person who created the breach will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will work with the Senior Head of IT to carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

## Appendix 2

## Use of Protective Marking

| | The information | The technology | Notes on Protect Markings (Impact Level) |
|---|---|---|---|
| School life and events | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils' work, lunchtime menus, extended services, parent consultation events | Publically accessible technology such as school websites or portal, emailed newsletters, subscription text services, mobile apps | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| Learning and achievement | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Via secure systems, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the Confidential (Level 1) category.<br>There may be students/ pupils whose personal data requires a HIGHLY CONFIEDENTIAL marking (Impact Level 2). For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way. |
| Messages and alerts | Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging or Learning Platforms or portals or mobile apps might be used to alert parents to issues. | Most of this information will fall into the CONFIDENTIAL (Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools' closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

## Appendix 3
## Data Subject Access or individual requests procedures

The following procedure should be followed if you receive a Data Subject or individual rights request as outlined in section 9. If you are verbally asked how a request should be made please direct them to https://thewhitehorsefederation.org.uk/gdpr alternatively if you personally receive a request via email or letter then the following procedure must be followed:

### All Staff

1. On receiving any request, please forward this to the DPO on the day it is received.

2. The DPO will log the request on the One Trust System, providing a response to the individual. The DPO may clarify finer details about the request with the school and the individual.

3. The DPO will verify the identity ID of the individual requesting the information.

4. The DPO will notify the Head Teacher and confirm what actions are to or have been taken.

5. The DPO will share a folder with a named individual from the school so that documentation can be shared securely. Documentation is not to be shared via email.

6. The DPO will scrutinize and redact the information to ensure that we are meeting our statutory obligations.

7. The DPO will ensure that the individual is kept informed and will share the information via the One Trust system.

### Verifying the identity of a Requester

The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

Where the DPO Lead has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

- Current passport
- Current driving licence
- Recent utility bills with current address
- Birth/marriage certificate
- P45/P60
- Recent credit card or mortgage statement

If the DPO Lead is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting to a data breach.

## Appendix 4
## CCTV Information

The CCTV system will operate continuously 24 hours each day of the year. The CCTV is sited at the following educational settings:

| Educational Setting | Camera Description | Number of Cameras | Capture sound? Yes or No | Move or Fixed |
|---|---|---|---|---|
| Devizes | X Vision | 70 | Some | Fixed |
| Drove | Hik Vision | 33 | No | Fixed |
| Forest & Sandridge | | 10 | No | Fixed |
| Gaglebrook | Hik Vision | 14 | No | Fixed |
| Gorse Hill | Cobra | 16 | No | Fixed |
| Grange Infants | Pyrotechnic | 4 | | Fixed |
| Grange Junior | Hik Vision | 9 | No | Fixed |
| Haydon Wick | CSA | 9 | No | Fixed |
| JMA | UNVR Avigilon | 53 | 21 | Fixed |
| Moak | Samsung SND-460V | 87 | No | Fixed and Move |
| Mountford Manor | Hik Vision | 16 | No | Fixed |
| Nyland | IVMS-4200 | 52 | No | Fixed |
| Ridgeway School | Hik Vision | 154 | No | Fixed |
| Rodbourne Cheney | Cobra | 14 | No | Fixed |
| Southbroom infants | Kalax | 4 | No | Fixed |
| Southwold Primary | Cobra | 7 | No | Fixed |
| St Luke's Academy | Honeywell | 68 | Some | Fixed |
| St Mary's & All Saints | Geovision | 16 | No | Fixed |
| The Croft | Hik Vision | 16 | No | Fixed |
| The Manor | Concept Pro Edge | 9 | No | Fixed |
| Tregoze | Hi Look | 15 | No | Fixed |
| West Kidlington | Hik Vision | 6 | No | Fixed |
| Whitelands | Hik Vision | 68 | No | Fixed |
| Zouch | | 6 | No | Fixed |

The images recorded by the CCTV cameras will not be actively monitored.
The images created by the system will only be accessed in response to reports of crime.

Each camera has an overwrite system that automatically deletes footage after a period of 30days. Recordings will only be retained if there is a specific purpose for which they are required to be retained for longer.

The system will be operated by site or office staff, it is checked on a day to day basis to ensure the images and recordings are of good quality.