White Trees independent school

part of the SureCare group

Data Protection Policy

Including GDPR updates and procedures

See also: Online Safety policy

Our vision is to provide pupils with the confidence, skills and ambition to achieve a successful and productive life. We aim to ensure they leave us with the opportunities and are able to become positive members of their communities. To do this, we have 3 principles that underpin our policies, practices and everything we do:

- Everyone can learn, achieve and has the potential to be successful
- Positive relationships are key to success and are underpinned by mutual trust, respect and caring for one another
- We have high expectations in everything we do

W onderful
E xcellent
L ovely
C lever
O utstanding
M agnificent
E nthusiastic

(Acronym created by White Trees pupils)

INTRODUCTION

White Trees 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, 2018). 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 school and educational bodies, and potentially social care services and the police. This policy is in place to ensure all staff, governors and directors are aware of their responsibilities and outlines how the organisation complies with the following core principles of the GDPR.

PERSONAL DATA

We acknowledge that there are many typed and categories of data and information that all require specific considerations around use and confidentiality.

- 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.

White Trees 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

White Trees 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 White Trees 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, White Trees 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 White Trees School is teaching, which does not 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 White Trees School qualifies as 'large scale' by a reasonable interpretation of the term,**

as measurements are not specified in legislation.

In contrast to the statutorily defined role and position of a DPO, White Trees School employs a more

flexible and equitable approach. All members of the school's leadership team 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 with responsibility lying with the Head Teacher and the Directors. 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.

Like a DPO, the data compliance officer will monitor the organisation's compliance with the GDPR. When deciding whether or not to appoint a DPO, White Trees School gave significant consideration to the guidance *Data Protection Officers and independent schools': guidance on whether to appoint*, published by Farrer & Co through the Independent Schools' Bursars Association in 2017.

DATA PROTECTION FOR PUBLIC EXAMS

This policy details how White Trees, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (DPA) and General Data Protection Regulation (GDPR).

Pupils are given the right to find out what information the school holds about them, how this is protected, how this can be accessed and how data breaches are dealt with.

All exams office staff responsible for collecting and sharing candidates' data are required to follow strict rules called 'data protection principles' ensuring the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

To ensure that the school meets the requirements of the DPA and GDPR, all candidates' exam information – even that which is not classified as personal or sensitive – is covered under this policy.

Section 1 – Exams-related information

There is a requirement for the exams office to hold exams-related information on candidates taking external examinations. For further details on the type of information held please refer to *Section 4 – Candidate information, audit and protection measures*.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority

This data may be shared via one or more of the following methods:

- hard copy
- email
- secure extranet site(s) – [e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services;]

This data may relate to exam entries, access arrangements, the conduct of exams and non- examination assessments, special consideration requests and exam results/post- results/certificate information.

Section 2 – Informing candidates of the information held.

White Trees School ensures that candidates are fully aware of the information and data held. All candidates are:

- given access to this policy via school website.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form (Personal data consent, Privacy Notice (AAO) and Data Protection confirmation) before access arrangements approval applications can be processed online.

Section 3 – Hardware and software

The table below confirms how IT hardware, software and access to online systems is protected in line with DPA & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Desktop computer	Individual Username and Passwords Umbrella security software Antivirus protection	Maintained by Head Office

Software/online system	Protection measure(s)
Google Drive	Individual usernames and passwords linked to staff email addresses. Only the Exams officer & SLT will have access to the Exams folder.
Awarding body secure extranet site(s)	Individual usernames and passwords Exams Officer has to approve the creation of new user accounts and determine access rights

Section 4 – Candidate information, audit and protection measures

For the purposes of this policy, all candidates' exam-related information – even that not considered personal or sensitive under the DPA/GDPR – will be handled in line with DPA/GDPR guidelines.

An information audit is conducted annually.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected.

Protection measures may include:

- password protected documents saved on the google drive in the EXAMS FOLDER
- secure drive accessible only to selected staff.

Section 5 – Access to information

Current and former candidates can request access to the information/data held on them by making an **access request** to Sarah Rixson, Exams Officer, in writing. ID will need to be confirmed if a former candidate is unknown to current staff.
Response to all requests will be actioned within one month.

Third party access

Permission should be obtained before requesting personal information on another individual from a third-party organisation.

Candidates' personal data will not be shared with a third party (see GDPR Policy) unless a request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties.

In the case of looked-after children or those in care, agreements may already be in place for information to be shared with the relevant authorities (for example, the Local Authority). The Schools Head Teacher will confirm the status of these agreements and approve/reject any requests.

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 and informed.
- Where consent is given, a record will be kept documenting how and when consent was given.
- White Trees 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 discontinue.
- Consent can be withdrawn by the individual at any time.
- The consent of parents/carers is sought prior to the processing of a child's data.

THE RIGHT TO BE INFORMED

- The privacy notice supplied to individuals in regard to the processing of their personal data is written in clear, plain language, which is concise, transparent, easily accessible and 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.
- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- In relation to data that is not obtained directly from the data subject, this information will be supplied:
- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

THE RIGHT OF ACCESS

- Individuals have the right to obtain confirmation that their data is being processed.
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- White Trees 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, White Trees 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, White Trees 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, White Trees 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

White Trees 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 White Trees School's 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. White Trees School will restrict the processing of personal data in the following circumstances:

- Where an individual contest 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.
- White Trees School will provide the information free of charge.
- White Trees School is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.

  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.
- White Trees 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

White Trees 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.

White Trees 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:

- White Trees School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- White Trees 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.

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. There are several steps and processes in place to support this handling of data breaches:

- 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 White Trees 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 trust 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 White Trees 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.
- The data that is stored on our cloud service and each individual's access is password protected.
- 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.
- 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 authentications 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.
- 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 White Trees 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.

White Trees 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

White Trees School makes only the following information routinely available:

- Policies and procedures

White Trees School will not publish any personal information, including photos, on its website without the permission of the affected individual. When uploading information to the school's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

PHOTOGRAPHY

- White Trees School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- White Trees School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- If White Trees School wishes to use images/video footage of pupils in a publication, such as the school's 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.

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 White Trees 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 GOOGLE CLOUD/DRIVE

- We use Google Cloud's Google Drive service as a sharing platform that provides secure, accessible storage across our school. Google are committed to leading on compliance with GDPR: h ttps://cloud.google.com/security/gdpr/ (Last accessed March 2018).
- Google Drive is very secure, and only those with an whitetrtees-school.com domain login can access the drive (and specific folders are available to individuals on a need-to-access basis, as decided by the Head Teacher). Information relating to child protection information is not held here.
- Google Drive is subject to EU Data protection laws as the servers are in operation around the world, the closest of which is in Dublin, Ireland. A list of data centres and information around the security of Google drive and other Google Apps can be found at this website address: h ttps://www.google.com/about/datacenters/ (Last accessed March 2018). The government's latest guidance on use of the cloud is here: h ttps://www.gov.uk/government/uploads/system/uploads/attachment_data/fil e /584755/Cloud_computing_services_guidance_Jan_2017.pdf (Last accessed March 2018).

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 school, **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.

INFORMATION REQUESTS (SEE APPENDIX 3)

- White Trees School will respond within 10 working days to any written or emailed request for information which they hold or publish
- The school will provide information on where to access the information required eg. the website link, o r details of a charge if the publication/ information is charged or send any free information. If the item is charged the school 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 school does 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 school 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 school owns the copyright – this is particularly important where the original publication was a charged item
- The school 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 Head Teacher. 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

- Employees are required to keep confidential about White Trees School's 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 school. Employees must not remove any documents or tangible items which belong to the school or which contain any confidential information from the school premises at any time without due cause. This includes the unauthorised use of any headed paper containing the school logo and/or contact details.
- Employees must return to the school if requested and, after consultation, and in any event upon the termination of your employment, all documents and tangible items which belong to White Trees 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 school' 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 school must not be passed on or made available to unauthorised persons within or external to the school.
- Employees who have access to the school' accounts and financial transactions are not permitted to disclose this information without the authorisation of the Head Teacher or governing body.

- Any confidential paperwork and documents are to be shredded using the office's cross shredder. This includes pupils and staff paperwork. The content is then able to be disposed of in a normal manner, due to the type of shredder we have.

RETENTION OF SCHOOL RECORDS AND PERSONNEL INFORMATION

School Records:

- Where a pupil is on roll with White Trees 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.
- Where a pupil comes off the White Trees School roll before the conclusion of year 11, their records (including CP/safeguarding files) will be forwarded securely to their new school.
- If the child is in their final year of education and qualifies as a Child Looked After, all records (including CP/safeguarding files) will be retained until the child's 75th birthday.
- If the pupil is in their final education year and they are not a child looked after, 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.
- If the child is in their final year of education and are not classified as child looked after, the pupil's records will be retained by White Trees 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:

- 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.
- 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.
- Unless there have been CP/safeguarding concerns, staff files will be retained for 6 years after the employee has left the employment of White Trees School.
- All physical files that are retained in accordance with the conditions outlined above are held in White Trees School's head office securely 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.

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 school' 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 school 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 school, 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
- school that a pupil attends after leaving White Trees School
- The Department for Education (DfE)
- NHS (including our commissioned school nurse)
- 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, eg. social care services, the police.

Personal data will not be retained by the school for longer than necessary in relation to the purposes for which they were collected.
White Trees 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 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, Laura Bull.

Withdrawal of consent

The lawful basis upon which the school process personal data is that it is necessary in order to comply with the school 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 ICO

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 ICO 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 school processes personal data is because it is necessary in order to comply with the school 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 school 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 school census and absence information.

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

- recruitment and employment purposes
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- to assist in the running of the school
- 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 school without your consent unless the law allow 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 h ttps://www.gov.uk/education/data-collection-and-censuses-for-school. For more information about the department's data sharing process, please visit: h ttps://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 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, Richard McCabe.

Withdrawal of consent

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

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 ICO 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 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 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
    - iP45/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 school may make a reasonable administration charge for the provision of information.
5. The response time for subject access requests, once officially received, is 10 working days.
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 school 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 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 (ICO).

Responding to subject access requests that may involve providing information relating to another individual (a 'third party individual')

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 ICO guidance.

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

APPENDIX 4

Data Protection Officers and independent school: guidance on whether to appoint

One of the areas of the General Data Protection Regulation (GDPR) which has resulted in the most confusion in school – and seen most mixed messaging from the many consultants and articles out there about GDPR – is the question of who will be caught by the new requirement for a mandatory Data Protection Officer (DPO), and what that title means.

The short answer – which may surprise some – is that independent school will not, in most cases, need to appoint one. The question of whether they ought to do so voluntarily is more complex. However, for reasons discussed below, adopting what might be seen as the most cautious or compliant approach (i.e. appointing a DPO in time for 25 May 2018) is not necessarily the safest route, let alone the most practical and commercial.

Appointing a DPO unnecessarily could be an expensive misstep, but many schools are confused about the role and what it entails. The Information Commissioner (ICO) has yet to put out guidance, while the existing EU working party guidance clearly does not consider the legal position of the UK independent school sector. For this reason, ISBA considers there is a clear need for a detailed note on the topic aimed at independent school.

1. **What do we mean – and not mean – by a DPO?**

This is an important issue to get straight at the outset. Under GDPR, a DPO may not be what you think it is.

As a point of best practice – or, frequently enough, operational necessity – many schools already have a "Data Protection Officer", or someone of similar title, who more often than not is the bursar. In times past this simply meant the person in charge of most data decisions and administration at the school, most notably dealing with subject access requests and other potential distractions.

Some school, in common with other organisations, erroneously refer to this person referred to as a "data controller" – a misunderstanding of a term that refers, in data protection law, to the school itself. Prior to 25 May 2018, by contrast, "Data Protection Officer" or "DPO" would be a very sensible job title to give that person, in line with both ICO terminology and market practice. However, as we shall see, calling anyone by that title after 25 May 2018 will carry a risk if the role is not intended to have the precise legal effect intended of it by GDPR.

The more formalised, carefully prescribed role of the DPO set out in the GDPR pushes an already unwelcome series of operational responsibilities and requirements to a higher level – and brings with it HR and accountability headaches. This is why school should think carefully before appointing a DPO, or even re-appointing the same person to the role, after 25 May 2018.

2. **Will your school legally require one?**

The ICO acknowledges (as it did at the ISBA Cyber Security conference in October 2017) that for independent school this position is by no means certain. Neither the GDPR wording nor the current EU working party guidance discloses a clear basis to suppose that most independent school would be intended to be caught by the strict requirement.

This is contrast to the much clearer position with maintained school, because all public authorities do indeed require a DPO. It may be that a single individual DPO will affix to the local authority as a whole

rather than to each school, according them a degree of independence (as well as being cheaper of course, allowing oversight of numerous maintained school): but this will depend on levels of access and capacity to deal with issues. As set out below, there may be lessons to learn for independent school in observing what works best.

(i) The position with independent school

For larger independent school, it may be a relief that the draft GDPR requirement based on sheer numbers has not made it into the final regulation – for a time, it looked like any organisation of more than 250 people would require a DPO. Instead, the test is one of use and volume. Either

(a) do your "core activities" consist of either large-scale, systematic or regular monitoring of individuals?; or

(b) do your "core activities" relate to large-scale processing of special category personal data? (e.g. health, sexual life, ethnicity, religion – broadly the old "sensitive" categories).

The key terms here are "core activity" and "large scale", and they are not further defined by GDPR. We are as yet lacking in clear and comprehensive guidance, but the EU working party guidance does draw some helpful conclusions. For example, it is the case that all employers are likely to process some special category data about their employees. However, while employing people is a necessary part of what they do, this does not make it their "core activity": it is ancillary to its main purpose.

A cautious analogy might be made to how school process personal data of parents and, most obviously, pupils. Safeguarding, for example, is a core obligation on school, and one which will properly involve both (a) the processing of sensitive personal data and (b) regular or systemic monitoring of staff and pupils. But the "core activity" of the school is education.

On balance, it might be safer to assume that a school's core activities *would* include processing special category data – but is it on a large scale? This is really where the DPO requirement looks less appropriate for most school. "Large scale" is not defined but it would appear intended to cover bigger corporations who do market analysis, private health, tech companies and so on: it is unlikely to cover school communities of a few hundred people.

Considerations for what sort of larger independent school could be caught might, however, include:

- Do you hold a large amount of alumni data, and do you either monitor them or hold significant volumes of e.g. safeguarding files or incident reports?
- Do you have particularly intrusive monitoring systems?
- Is your school part of a large trust or multi-school business model where the "data controller" is likely to be the ultimate proprietor, i.e. the trustees or top company board?

If so, you might be looking at "large scale" processing activity of the sort that fits into either category, and consider the appointment of at least a single DPO for the entire group (where applicable). But until the ICO gives clear guidance on the topic, and lends some quantifiable measure to "large scale", there is something to be said for watching and waiting.

(ii) Comparison with other types of school

It will be of interest for the private school sector to watch how the best practice position develops not

simply with the 'traditional' state sector and academies, but also with more comparable models such as free school and multi-academy trusts. These would qualify as public authorities, and require a DPO (albeit they are not always on all fours with maintained school in how they are treated for certain other requirements of information law – e.g. a parent's right to see the pupil file).

Structurally, and in terms of independence of decision making from local authorities (a key characteristic of a data controller being who actually determines what is done with personal data), such school would seem to have more in common as data controllers with independents. Therefore, independent school should be vigilant as to developments elsewhere in education – even if they decide not to make the initial formal DPO appointment. It will be salutary to learn which DPO models work best in practice, especially for groups of school, and which are less effective (or likely to have unintended consequences).

3. **What are the expectations of the new DPO role?**

Notwithstanding the lack of certainty in the law – or perhaps because of it – some school are considering appointing a DPO voluntarily. Whether or not you are required to appoint a DPO by law, if you do appoint one then the following applies:

- **The DPO must possess "*expert knowledge of data protection law*".**

This, notably, is not a requirement of IT expertise (although that might help!) but refers to a legal and practical understanding of how the law protects the privacy rights of individuals. GDPR values that over digital skills, and this seems particularly important in a school context.

- **The DPO must be *properly*, and *promptly*, *involved* in all issues related to the protection of personal data at the school.**

This runs from policy (at the outset) and overseeing privacy impact assessments, to dealing with requests from individuals (e.g. subject access) and whether and how to report data breaches to the ICO (which is mandatory within 72hrs if a certain threshold is reached) or affected individuals. Ultimately these decisions are for the school to make as data controller – hence the requirement for the DPO to be "*properly* [i.e. meaningfully] *involved*", i.e. to advise and inform, rather than having fully delegated responsibility.

- **The DPO can be an existing member of staff, or appointed to take on more than one role: being DPO does not have to be his/her sole responsibility…**

This is consistent with the idea of course that a school can make an external appointment, or that one person can be DPO to several school – provided there is sufficient access, in both directions, in each case (and sufficient independence from the interests of the governors / trustees / top company).

- **…however, a DPO must take sole responsibility for that role.**

Responsibility is not the same as liability (rather the opposite – as explained below, the liability is ultimately with the school). What this means is that you cannot share the role across two or three staff members: the ICO expects a single person as their point of contact.

This is in contrast to a more flexible team approach if your school does not make the formal appointment. Either way, depending on the size of your school, you may want data "champions" across several relevant departments (*administration / governance, IT, development, archives, legal/compliance, safeguarding, teaching staff etc.*) to assist the role.

- **The DPO must be independent, not too senior or conflicted…**

EU working party guidance is clear that senior management, and specifically the heads of key departments like IT and HR, could be too conflicted to carry the role effectively and objectively. Similarly, bursars (and head teachers) are likely to be too aligned in their interests with the school to qualify: a DPO must speak truth to power, and make recommendations often against the organisation's short-term reputation or commercial interests.

- **…however, the DPO must have clout within the organisation.**

They need to report to the highest level of management – the head, bursar and governors – and organisations are legally obliged to give them support, access, training and resources. As a compliance requirement, a DPO must be appointed "*on the basis of professional qualities*" and not simply appointed within the organisation based on who is willing to take on the role.

Therefore school might understandably wonder who at their organisation could possibly qualify, and indeed what they might expect to be paid on top of their existing salary.

- **The DPO's independence is protected at law.**

  Ultimately the DPO's duties are as much to the ICO and to the public (the school's "data subjects") as they are to the school. GDPR states that DPOs *"shall not be dismissed or penalised… for performing his* [or her] *tasks"* – something approaching "whistle-blower" type protections – and should not "*receive any instructions*" in how to carry out those tasks.

In practice that definition of "instructions" may need to be explored: as above, it is ultimately for the data controller (school) to make decisions about whether to report a breach, disclose or amend a record, agree the terms of a contract with a data processor (e.g. cloud service provider), or go ahead with a major IT revamp or fundraising campaign. But the practical consequences of leaning on a DPO not to disclose something under a subject access request or ignoring a recommendation (e.g. concerning breach reporting or the impact of a new measure) could be serious in enforcement terms.

- **The DPO has considerable record-keeping responsibilities.**

This is not only a practical burden on the individual, but it is a core part of the accountability aspect of a school's GDPR compliance. Ultimately, if the school goes ahead with a major new project that might impact on individual privacy (e.g. marketing, CCTV, or monitoring), there should be a paper trail evidencing that this was thoroughly considered; and if a school has taken advice against a DPO's recommendation, the fact ought to have been recorded. The ongoing duty to assess and record the privacy impact of a decision continues even after the event.

- **When appointed, the DPO's details must be published and notified to the ICO.**

The DPO's task includes a duty to "*cooperate with the supervisory authority*". One of the key tensions of the role is likely to be how the DPO balances duties to his or her paymaster with those to the regulator.

In summary, therefore, although designed to improve data protection practices at an organisation, the role of DPO brings with it considerable compliance and operative burdens in itself. For organisations like school that are relatively small but extremely complex, and lacking substantial resources, it may be more attractive to adopt a more flexible approach than diving in to appoint a DPO.

4. **If we decide not to appoint a DPO, what *do* we have to do?**

As above, the ICO has not issued a clear position on DPOs and independent school. Where the ICO is clear, in which regard ISBA and its lawyers are fully in agreement, is that any school will need to appoint a suitably trained, capable and competent person to take on the role of compliance lead at the organisation.

This person will require knowledge of data protection law, as well as being plugged in to the culture and structure of the school. In any event, the record keeping and accountability requirements of GDPR (as merely hinted at above) will need to be in place whether or not the person leading the charge is called a "DPO". So in fact, a school would want to go most of the way to appointing a role with all the qualities – and many of the responsibilities – of a DPO.

In doing so, the school would be well positioned to "flip" the role to a more formal appointment in the event that the ICO decided, down the line, that the Article 37 GDPR (the relevant section) had the effect of catching independent school; or that such an appointment was always good practice in the sector; or if your school grew in size, or changed in structure, or started intensive monitoring. But there is a clear attraction in the meantime in waiting to see how the position pans out for others.

There is also a benefit in not having to appoint a new role; or allowing an outsider to have access to the school's most sensitive systems; or notably increase the burden and complexity of a valued existing employee's role. That is especially so, given the highly competitive employment market for individuals qualified to take on the DPO role (as either a full-time position or consultant) – and indeed the conflicting requirements about the person's required level of seniority, which does not lend itself well to an organisation the size of the average independent school.

5. If we are not appointing a DPO, what do we call them?

EU working party guidance is clear that to appoint anyone in a compliance lead role who is not intended to be a DPO, it must be clear to all (the public and the ICO) that this is indeed not intended. Calling them a DPO, or anything too close (School DPO, Officer for Data Protection, Data Processing Officer etc.) is therefore unwise and could well have the effect of requiring compliance to the high GDPR standard.

Consider more imaginative (but descriptive) variations like Compliance Officer (Data), Privacy Officer, Head of Data Protection and so on.

Published on	
By	
Chair of Gov Sig/Date	
Head Teacher Sig/Date	

Staff read and acknowledged:

Name	Sig/Date

