CAWOOD CHURCH OF ENGLAND (VA)

PRIMARY SCHOOL

Information Security policy

(April 2020)

Document Status			
Date of next review	April 27th 2021	**Responsibility**	Finance and Staffing Committee
Date of Policy Creation Version 1	April 2020	Reviewed annually	
Date of Policy Adoption by Governing Body 27.4.2020		**Responsibility**	Chair of the Finance and Staffing
Reviewed		**Signed**	
Method of Communication			
Website, Server			

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Cawood Primary's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Information Security Policy outlines the School's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 270001 (internationally recognised information Security standard).

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework with particular focus on the Acceptable Use Policy and the Information Security Incident Reporting Policy.

Scope

All policies in the Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors.

Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

Access Control

The School will maintain control over access to the personal data that it processes.

These controls will differ depending on the format of the data and the status of the individual accessing the data. The School will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the admin officer.

Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use.

Keys to storage units will also be locked away. The admin officer will be responsible for giving individuals access to the key safe. Access will only be given to individuals who require it to carry out legitimate business functions.

Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two tier authentication system will be implemented across all electronic systems. The two tiers will be username and unique password.

Individuals will be required to change their password every term and user names will be suspended either when an individual is on long term absence or when an individual leaves employment of the School.

Software and Systems Audit Logs

The School will ensure that the main software and systems (such as the server, Scholar pack and O track have inbuilt audit logs so that the School can ensure it can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the

integrity of the data can be assured and also deters individuals from accessing records without authorisation.

The school is accountable for the data it holds in school. The school moved from Sims to Scholarpack in April 2020.

Here is hoe Scholarpack maintains good information security.

ScholarPack GDPR Guide

This guide has been designed to answer all of your questions relating to GDPR and ScholarPack.

Is ScholarPack GDPR compliant?

Yes, and we have engaged an external company that specialise in data governance and privacy to assist us in complying with the General Data Protection Regulation (GDPR). We are already accredited under the ISO 27001 Information Security framework and are working with our advisors to identify any improvements based on the GDPR expectations should they be required in advance of the aforementioned date.

How do you use our data?

As a Data Processor we commit to only storing and displaying the information you provide. We do not use it for any other purpose.

Where exactly does ScholarPack store our data?

School data is held in secure Tier 4 data centres within the UK that are protected by both physical and logical security, and conform to industry standard security practice. Our live systems and backup systems are hosted with different providers in different geographical locations within the UK.

What access does ScholarPack have to our data?

Access to schools' data is strictly controlled and monitored at ScholarPack, and we employ a 'least privilege' code of practice within our organisation. We have various security procedures in place which ensure the safety of your data within our ISO 27001 system, and the database is only accessed with express permission from the school.

How is my data backed up?

School data is mirrored in real time to a standby server by 'streaming replication'. This means that we always have an up to date backup ready to take over should there be problems with the primary serve and a formal back up is taken daily. These backups are then moved to high availability, replicated data storage across three geographically separate data centres to mitigate against the failure of the primary data centre.

Is the data encrypted in transit and at rest?

ScholarPack uses industry standard encryption to protect user and student data in transit and at rest.

How long does ScholarPack hold data / What is ScholarPack's data retention policy?

Currently all student and staff data will remain on the system unless deleted by yourselves or you move to a different MIS supplier. All backups are held for six months. ScholarPack will work with schools to implement their data retention policy.

If you do delete a student via the extended tab (you may do this if they were meant to attend your school and never turned up, for example) then this data will be completely removed. We do have backups which are held for 6 months, and data deleted from the live school will not be removed from the backup during this time.

Does our ScholarPack contract comply with the new GDPR?

Schools who are currently under contract will be receiving a GDPR Compliance Variation to replace the current Schedule 3 in the contract. If a school is awaiting a new contract then there will be a version with an updated statement.

Are there any instances where our data is passed to other organisations outside of ScholarPack's sub processors?

We have API links with several organisations in order to sync up your data with different companies you may use within your school. These are set up exclusively within the school by the SysAdmin user. No other data is shared with any other companies, and the data made available via each API can be viewed in the API Config page in ScholarPack.

How does ScholarPack ensure the safety of our data through the vetting of employees?

Each ScholarPack employee is required to hold an enhanced DBS and comply to company regulations on data sharing and confidentiality. They are trained in strict compliance to ISO 27001 and receive monthly refresher training to ensure retention and active practice.

If I receive a request of All Data Held on a child in my school - what do I need to do?

Should this request occur we are happy to prepare this data. However, please note that this may take a period of time to collate, the time needed would be dependent on the specificity level of the required data. Once you have further clarification from the parent on what information they require, please send an email from the Headteacher's school email account requesting this data for the student with the correct student ID number.

How is data transferred between 3rd Parties and ScholarPack using the API?

Our API links are over SSL encrypted HTTPS and we enforce that it cannot be accessed through any other route.

How does ScholarPack deal with data breaches?

ScholarPack takes the security and consistency of users data very seriously. If we become aware of a breach, we will work to ascertain the limits of such breach and notify affected Schools as soon as we become aware who those Schools are. We will work with the schools to communicate with affected parties, and determine if such a breach should be reported to ICO.

Where a breach is reportable we will work with affected schools Data Protection Officer to help submit the declaration and manage the enquiry.

Who can authorise the destruction of any data on ScholarPack? How does ScholarPack dispose of IT hardware?

The systems operations team can undertake the deletion of this data if requested by the school. Single records can be deleted from the front end system by the Sysadmin user. All data that is erased is non recoverable and overwritten immediately. Any data storage media that is taken out of service is securely destroyed and we maintain certificates of each piece of hardware processed in this way.

What internal audits are in place to ensure that there is no unauthorised access of ScholarPack data?

ScholarPack records all user logins to schools and these are regularly audited at an operating system level. We have systems and processes in place to monitor unauthorised access to ScholarPack. If a school notifies us of suspicion of unauthorised access, we can work with the school to verify the log ins and provide a historical audit. We provide several mechanisms for limiting locations from which users can log into ScholarPack.

Does anyone within your organisation have access to the personal information of the Data Controller?

ScholarPack employees only have access to the personal information of the Data Controller with the express permissions from the school to undertake maintenance and support activities, and access is audited.

What Subprocessors and 3rd Parties does ScholarPack use?

We use a number of Sub-processors in order to deliver services such as email, SMS and backups. A full list is available here

Do ScholarPack contracts of employment contain confidentiality and gross misconduct clauses, in the context of customers data privacy?

Our employee contracts are GDPR compliant.

Does The Key have access to school data?

No, the data access stays exactly the same. Schools are the data controllers and ScholarPack are their data processors, this relationship is unchanged.

O Track Information security

We have taken significant steps to ensure that we process personal data in compliance with the General Data Protection Regulation (GDPR). Further information can be found about the steps we have taken to become GDPR compliant at https://optimumotrack.co.uk/otrackand-gdpr/

OTrack – Privacy Policy

INTRODUCTION
Welcome to the Optimum Reports Limited's t/a Optimum and OTrack (“Optimum”, “we”, “our” and “us”) privacy notice.

Optimum respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

We have taken significant steps to ensure that we process personal data in compliance with the General Data Protection Regulation (GDPR). Further information can be found about the steps we have taken to become GDPR compliant at https://optimumotrack.co.uk/otrackand-gdpr/

1. IMPORTANT INFORMATION AND WHO WE ARE

Purpose of this privacy notice

This privacy notice aims to give you information on how Optimum collects and processes your personal data through the use by an educational establishment of our software (“OTrack”) which is accessed via https://login.otrack.co.uk (in conjunction with any other websites we may publish from time to time, the “Website”). This personal data includes any data you may provide through the Website when you sign up to our newsletter or purchase OTrack from us.

We collect and process personal data relating to children which is uploaded by those persons using OTrack on behalf of educational establishments (referred to herein as “Users”) as part of their use of OTrack.

Controller / Processor

Optimum is the controller of personal data collected and processed about Users, persons who sign up to our mailing list, individuals at our suppliers and partners, our employees and persons who have indicated that they wish to book a demo of OTrack or have otherwise requested further information about OTrack (“Leads”). This privacy statement relates only to our processing of personal data in respect of Users, Pupils and Leads.

We are a data processor in respect of personal data provided to us by Users in respect of pupils of the educational establishment (“Pupils”).

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the Data Protection Officer at **O track** (DPO) via the school office. (01757 - 268368)

Third-party links

The Website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements.

2. . THE DATA WE COLLECT ABOUT DATA SUBJECTS

“Personal data”, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed such that the identity of the person to whom the information relates can no longer be ascertained (anonymous data).

We may collect, use, store and transfer different kinds of personal data about data subjects which we have grouped together as follows:

Personal data relating to Users

Identity Data includes first name, last name, username or similar identifier, marital status, title, DfE number and job title.

Contact Data includes school name, billing address, email address and telephone numbers.

Financial Data includes bank account and payment card details.

Transaction Data includes details about payments to and from the User and other details of licences and services the User has purchased from us.

Technical Data includes internet protocol (IP) address, the User's login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access the website.

Profile Data includes the User's username and password, purchases or orders made by the User, feedback and survey responses.

Usage Data includes information about how the User uses the Website and OTrack.

Marketing and Communications Data includes the User's preferences in receiving marketing from us and our third parties and the User's communication preferences.

Personal data relating to Pupils

Identity Data includes first name, last name, username or similar identifier, title, FSM6 status, date of birth, year group, class group, photograph, gender, ethnicity, attendance summary, SEN status, SEN need, FSM status, pupil premium status, EAL status, in LEA care status, ever in care status, gift and talented status, school entry date and UPN.

Personal data relating to Leads

Identity Data includes first name, last name and local authority where the educational establishment is based.

Contact Data includes email address and telephone number.

We also collect, use and share "**Aggregated Data"** such as statistical or demographic data for a number of purposes. Aggregated Data may be derived from personal data but is not considered personal data in law as this data does not directly or indirectly reveal the identity of the data subject. For example, we may aggregate Usage Data to calculate the percentage of Users accessing a specific Website feature. However, if we combine or connect Aggregated Data with a User's personal data so that it can directly or indirectly identify the User, we treat the combined data as personal data which will be used in accordance with this privacy notice.

"Special Categories of Personal Data" includes details about a person's race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data.

We process the following Special Categories of Personal Data in respect of Pupils only: (incidentally) health data.

3. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about data subjects including:

Direct interactions. Users may give us their Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data provided by Users when they:

- create an account on the Website; - subscribe to OTrack; - request marketing to be sent to them; - enter a competition, promotion or survey; or - give us some feedback.

Users may also provide us with Identity Data relating to Pupils via OTrack.

Leads may provide us with Identity and Contact information when they request a demo or otherwise indicate an interest in OTrack.

Automated technologies or interactions. As Users interact with the Website, we may automatically collect Technical Data about the User's equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. Please see our cookie policy for further details.

Third parties or publicly available sources. We may receive personal data about Users from various third parties as set out below:

Technical Data from the following parties:

- analytics providers such as Google; - advertising networks; and - search information providers.

Contact, Financial and Transaction Data from providers of technical and payment services.

Identity and Contact Data from publicly availably sources such as Companies House and the Electoral Register.

4. HOW WE USE YOUR PERSONAL DATA

We will only use personal data when the law allows us to. Most commonly, we will use personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with a User. - Where it is necessary for our legitimate interests (or those of a

third party) and the interests and fundamental rights of the User and/or Pupil do not override those interests. - Where we need to comply with a legal or regulatory obligation.

For further information about the types of lawful basis that we will rely on to process personal data, please see the Glossary at section 10 below.

Generally, we do not rely on consent as a legal basis for processing your personal data other than:

- In relation to sending direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

- In relation to processing Special Categories of Personal Data in respect of Pupils in respect of which the parent or guardian of the relevant Pupil must have given (and not withdrawn) consent.

5. PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process personal data for more than one lawful ground depending on the specific purpose for which we are using personal data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register a User as a new customer	(a) Identity (b) Contact	Performance of a contract with the User
To process and deliver a subscription for OTrack including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with the User (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with the User which will include: (a) Notifying the User about changes to our terms or privacy policy (b) Asking the User to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with the User (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how Users use our products/services)
To enable the User to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with the User (b) Necessary for our legitimate interests (to study how Users use our products/services, to develop them and grow our business)

To administer and protect our business and the Website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to Users and Leads and measure or understand the effectiveness of the advertising we serve to Users and Leads	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how Users use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve the Website, OTrack, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep the Website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to Users and Leads about goods or services that may be of interest to them	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)
To record information about Pupils input by the User and to allow User(s) to access such personal data	(a) Identity	Performance of a contract with the User Subject to the consent of the parent / guardian of the Pupil

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.

You will receive marketing communications from us if you have requested information from us or purchased OTrack from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time by logging into the Website and checking or unchecking relevant boxes to adjust your marketing preferences or by following the opt-out links on any marketing message sent to you or by contacting us at any time.

Where you opt out of receiving these marketing messages, we will still send you communications relevant to the performance of our contract with you.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our Website may become inaccessible or not function properly. For more information about the cookies we use, please see our cookies policy which can be found on the Website.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share User and Pupil personal data with Third Parties as set out in the Glossary for the purposes set out in the table in paragraph 5 above. We require all third parties to respect the security of personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use personal data for their own purposes and only permit them to process personal data for specified purposes and in accordance with our instructions.

In the event that we sell, transfer, or merge parts of our business or our assets, the buyer will receive personal data in respect of Users and Pupils but shall only be permitted to use such personal data for the purposes set out in the table in paragraph 5 above. Alternatively, we may seek to acquire other businesses or merge with them.

7. INTERNATIONAL TRANSFERS

Some of our third-party processors are based outside the European Economic Area ("EEA") so their processing of personal data will involve a transfer of data outside the EEA.

Whenever we transfer personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We transfer personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.

- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

8. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify the relevant User and any applicable regulator of a breach where we are legally required to do so.

9. DATA RETENTION

How long will we use personal data for?

We will only retain personal data relating to Users for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. We will delete all personal data relating to Pupils on request by any User from the educational establishment responsible for uploading the relevant personal data, or from the Pupil, or the Pupil's parent or guardian.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which we process the personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about Users (including certain Contact, Identity, Financial and Transaction Data) for six years after they cease being Users for tax purposes.

In some circumstances you can ask us to delete your data: see the paragraph titled "Request Erasure" in section 9 below for further information.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

10. THE LEGAL RIGHTS OF DATA SUBJECTS

Under certain circumstances, data subjects have rights under data protection laws in relation to their personal data.

Each User, Pupil and Lead has the right to:

Request access to personal data held about them (commonly known as a "data subject access request"). This enables the data subject to receive a copy of the personal data we hold about him and to check that we are lawfully processing it. Where you are a Pupil, or the parent of guardian of a Pupil, we may request evidence of your identity prior to providing you with your personal data.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. We will always delete personal data in respect of any Pupil where we are requested to do so.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms. We will always stop any processing activity in respect of personal data of any Pupil where we are requested to do so.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you. So long as you can demonstrate that you have appropriate authorisation to enable us to transfer personal data relating to any Pupil, we will do so.

Withdraw consent at any time where we are relying on consent to process any categories of personal data. However, this will not affect the lawfulness of any processing carried out before consent is withdrawn.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

11. GLOSSARY

Lawful Basis

“Legitimate Interest” means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain

further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

“Performance of Contract” means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

“Comply with a legal or regulatory obligation” means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

Third Parties

- Service providers acting as processors who provide IT and system administration services.

- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.

- HM Revenue & Customs, regulators and other authorities acting as processors based in the United Kingdom who require reporting of processing activities in certain circumstances.

(End of O track Privacy Policy)

Data Shielding

The School does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the School.

The School will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and any electronic files will be locked down so that the declaring employee cannot access that data.
Employees who knowingly do not declare family and friends registered at the School may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access
On occasions the School will need to allow individuals who are not employees of the School to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a Partnership arrangement with another School. **The Headteacher** is required to authorise all instances of third parties having access to systems. If the above

individual is not available to authorise access then access can also be authorised by **The Assistant Headteacher.**

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the School.

Physical Security

The School will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the School:

Clear Desk Policy
Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

Alarm System
The School will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

Building Access
External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The caretaker will be responsible for authorising key distribution and will maintain a log of key holders.

Internal Access
Internal areas that are off limits to pupils and parents will be kept locked and only accessed through pin numbers or keys. Pin numbers will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a pin-operated key safe or a secure key safe.

Visitor Control
Visitors to the School will be required to sign in a visitor's book and state their name, organisation, car registration (if applicable) and nature of business. Visitors will be escorted throughout the School and will not be allowed to access restricted areas without employee supervision.

Visitor books will be locked away at the end of the working day and kept for current financial year + six years.

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the School must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of School but the School will implement the following mitigating controls:

Back Ups
The School will back up their electronic data and systems every day. These backups will be kept off site by an external provider. This arrangement will be governed by a data processing agreement. Should the School's electronic systems be compromised by an environmental or natural hazard then the School will be able to reinstate the data from the backup with minimal destruction.

Fire Proof Cabinets
The School will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises.

Fire Doors
Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.
Fire Alarm System
The School will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems Security

As well as physical security the School also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the School's ability to operate and could potentially endanger the lives of its Pupils.

The School will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions
Employees must request authorisation from JP Consultancy, before downloading software on to the School's IT systems. JP Consultancy and/or North Yorkshire ICT support will vet software to confirm its security certificate and ensure the software is not malicious. The school/ JP Consultancy will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

Phishing Emails

In order to avoid the School's computer systems from being compromised through phishing emails, employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with JP Consultancy and/or North Yorkshire ICT if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software
The School will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The School will update the firewalls and anti-virus software when updates are made available and when advised to do so by JP Consultancy and/or North Yorkshire ICT**.** The School will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Cloud Computing
The school uses sharepoint on an I cloud and Scholarpack which is a data management system.

IT IS RECOMMENDED THAT YOU ONLY ALLOW CLOUD COMPUTING IF THE SERVERS ARE HELD IN THE EUROPEAN ECONOMIC AREA OR ON YOUR LOCAL SERVERS.

Shared Drives
The School maintains a shared drive on its servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. For example a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The ICT support and the admin officer will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the School's retention schedule.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the School and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The School has implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by post
When sending personal data, excluding special category data, by post, the School will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post
When sending special category data by post the School will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email
The School will only send personal data and special category data by email if using a secure email transmission portal. The school uses Egress Switch for this purpose. Staff will add a layer of security by encrypting the email with a password.

Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

Exceptional Circumstances
In exceptional circumstance the School may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function
When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then School employees will utilise the Blind Copy (BCC) function.

Remote Working

It is understood that on some occasion employees of the School will need to work at home or away from the School premises. If this is the case then the employees will adhere to the following controls:

Lockable Storage
If employees are working at home they will ensure that they have lockable storage to keep personal data and School equipment safe from loss or theft. If the Employee does not have access to lockable storage then they may apply to the School for assistance in purchasing such storage.

Employees must not keep personal data or School equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or School equipment in cars if unsupervised.

Private Working Area
Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use School equipment for their own personal use.

Trusted Wi-Fi Connections
Employees will only connect their devices to trusted Wi-Fi connections and will not use ‘free public Wi-Fi’ or ‘Guest Wi-Fi’. This is because such connections are susceptible to malicious intrusion.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from JP Consultancy and/or North Yorkshire ICT.

Encrypted Devices and Email Accounts
Employees will only use School issued encrypted devices to work on Personal Data. Employees will not use personal devices for accessing, storing, or creating personal data. This is because personal devices do not possess the same level of security as a School issued device.

Employees will not use Personal email accounts to access or transmit personal data. Employees must only use School issued, or School authorised, email accounts.

Data Removal and Return
Employees will only take personal data away from the School premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.
Employees will ensure that all data is returned to the School premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.