Data Protection and IT Security Policy

Seva School are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Seva School collects and processes in accordance with the General Data Protection Regulation (GDPR). This policy sets out how we handle the personal data of our pupils, staff, parents and third parties and the precautions we take in order to protect this data. All members of staff and contractors are required to familiarize themselves with the content of this policy and adhere with the provisions set out in it. Failure to comply with this policy is considered an offence which may result in disciplinary action, according to the school's disciplinary policy.

Data Protection Regulations Act (2018)

The Data Protection Regulation 2018 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Key Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, personal image, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject – any living individual who is the subject of personal data held by an organisation.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory

authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child - Although, in the UK a child is considered to be anyone aged under 18, if you are relying on consent as your lawful basis for processing, in the UK the child may provide their own consent when they are aged 13 or over. If the child is under 13, any consent required will need to be obtained from the parent or custodian.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Data Protection Impact Assessment (DPIAs) – DPIA's are a tool used to identify risks in data processing activities with a view to reducing them.

Seva School adhere to the key principles of GDPR when processing personal data, as detailed below.

1. Personal data must be processed fairly and in a transparent manner where we have a lawful basis to do so;
2. Personal data must be collected only for specified, explicit and legitimate purposes;
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Personal data must be accurate and, where necessary, kept up to date;
5. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
6. Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

In order to achieve this Seva School has implemented the following policies and processes which must be adhered to at all times.

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

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

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust board

The school's policies and procedures are compliant with all relevant data protection obligations.

5.2 Data protection officer

The Data Protection Officer is Jo Holloway (Azteq) who is responsible for reviewing this policy, monitoring our compliance with data protection law, and assisting with developing related policies and guidelines where applicable.

The DPO will undertake an annual review of compliance and provide a gap analysis and advice on closing these gaps.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is contactable via joholloway@azteq.com

Jasvinder Kaur is the Data Protection Liaison at school.

5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the area encompassed by the United Kingdom and European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

When contacting the DPO directly, staff should also send a copy of their initial communication and then any subsequent correspondence to the Headteacher for the school's records and information.

No member of staff who raises genuinely held concerns regarding a possible data breach in good faith under this procedure will be dismissed or subjected to any detriment as a result of such action, even if the concerns turn out to be unfounded. Detriment includes unwarranted disciplinary action and victimisation. If the individual believes that s/he is being subjected to a detriment within the workplace as a result of raising concerns under this procedure, s/he should inform the Headteacher immediately. Workers who victimise or retaliate against those who have raised concerns under this policy will be subject to disciplinary action.

Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients,

how and why we are storing the data, retention periods and how we are keeping the data secure

Information Asset Register

Seva School has established a data inventory and data flow process as part of its approach to address risks throughout its GDPR compliance project. The Information Asset register determines

1. The data held by the school
2. Who has access to the data and how access is controlled
3. The content and purpose of data
4. Who this data is shared with
5. Legal basis for lawful processing
6. Details of consent where needed
7. Data Retention periods and schedules
8. Third party details of people we share data with
9. Data Protection Impact Assessments

Operations Manager is responsible for the maintenance of this register and this will be reviewed on a regular basis by the DPO.

Sharing data with Third Parties

Seva School will not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include–

1. The third party requires the information in order to carry out the contracted service
2. Sharing the data complies with the published privacy notice and if required, consent is obtained.
3. The transfer complies with any applicable cross-border transfer restrictions
4. The third party has signed a non-disclosure agreement.

Data Subject Rights and Requests

All school employees must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends etc. Staff should exercise caution when asked to disclose personal data on an individual. Data Subject Access Requests must be actioned in line with Seva School's data subject request procedures. Please see the *Data Subject Request procedures* for more detail.

Training

The school will ensure that all staff that handle data have undergone adequate training to enable them to comply with privacy laws and this training will be refreshed at least annually. All new starters will also undergo data protection and IT security training. The school will also ensure that after the termination of employment, staff and contractors are debriefed on their post-employment confidentiality responsibilities.

Staff should also familiarise themselves with our *privacy statement* on Sevak Privacy Statement for more information on how we handle data.

Data Protection Officer (DPO)

Our Data Protection Officer (DPO) is responsible for monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding DPIAs and acting as a contact point for data subjects and the supervisory authorities.

If you have any questions about the operation of this policy or the GDPR or if you have any concerns about the protection of data within the organisation, please contact the DPO –

DPO: AzteQ Group Ltd

Address: AzteQ House, Maxted Corner, Eaton Road, Hemel Hempstead, HP2 7RA

Telephone: 01442 244444

Email: SEVASchool-DPO@azteq.com

In the event of a data breach/suspected data breach, you should contact your DPO **immediately**.

For more information on this, please see the *data breach procedure*.

IT SECURITY POLICY

Seva School has taken many steps to ensure the security of our IT systems and protect the data within it. Ekte is responsible for the management of our IT security and we have implemented various processes to ensure that a high level of security is maintained. All IT systems are secured using up to date AV and malware, security and critical patches are installed within 14 days of release, a software firewall is running on all devices with access to school information and a hardware file is in place preventing unauthorised access to the school network.

We ask staff to ensure that when dealing with sensitive or confidential information they ensure that it is secured and stored appropriately. If you are unsure on the classification of data, how and where it should be stored then please check with Operations Manager.

User Access

In the case of new employees, the data access requirements must be detailed by the relevant department and sent to HR who will action this with Ekte as part of a new user set up. No accounts are to be set up with more access rights than necessary for the position. For more information on this matter, please refer to the *joiner/leaver process.*

Any changes in access rights must be approved in writing by the Principal.

A users account and access rights will be deleted immediately after a member of staff leaves. Their data will have previously been archived to a folder only accessible to the Principal. The email account will be retained for 30 days (subject to review) with the password changed and mail forwarded to a relevant member of staff.

To ensure all security policies are being followed and obligations met, quarterly network scans and an annual security review are carried out and these will be reviewed as part of the board meeting.

To ensure user access is not breached, all computers and electronic devices should be locked when not in use. You must immediately inform Operations Manager of any security concerns relating to IT systems which could or has led to a data breach.

Any other technical problems that could compromise data (such as hardware errors) should be reported to Helpdesk@seva.coventry.sch.uk.

Network

The security of our network is of upmost importance and Seva School have taken the following steps to maintain this.

1. Network passwords are always changed from the default upon initial configuration.
2. Passwords on all routers or hardware firewall devices are at least 8 characters in length and in line with the password guidelines.
3. The password on the router or switch is kept in a secure encrypted location.

4. Firmware will be updated on network equipment where vulnerabilities and threats have been identified as part of our regular network equipment and security scans.

We ask that our staff take the following steps in order to help us maintain our network security

1. Any devices not commissioned by Seva School should not access the internal network and use the guest network only.
5. IT will attempt to maintain appropriate filtering methods, but if you come across any unsuitable sites, this should be reported to IT immediately.
6. Staff should not attempt to gain access to restricted areas of the network or to any password protected information unless they are specifically authorised to do so.
7. Misuse of the computer system may result in disciplinary action. If you are unsure if your actions may constitute misuse them please check with IT before proceeding.
8. Staff are forbidden from accessing, from the school system, any web page or files which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While it may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. Staff must not use the school network to access chat rooms or internet message boards. Anyone found accessing inappropriate, offensive or distasteful content on the internet will be open to disciplinary action, up to and including dismissal.

Monitoring

1. The contents of our IT resources and communication systems are the Seva School's property. Therefore, staff should have no expectation of privacy in any message, files, data, social media post or any other kind of information or communication transmitted to, received, printed from or stored or recorded in our electronic information and comms systems.
2. Seva School reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media posting and activities, to ensure that out rules are being complied with and for legitimate business purposes. You consent to such monitoring by your acknowledgement of this policy.
3. The school may store copies of such data or communications for a period of time after they are created and may delete such copes from time to time without notice.

Hardware and Software

The purpose of this policy is to standardize and define the usage and setup of hardware and software within Seva School. A set of standards have been implemented to "harden" the equipment giving it greater protection from cyber-attack.

Hardware/Devices

1. Before purchases are made, all IT systems are assessed by Ekte and deemed suitable for compliance with school's security requirements.
2. It is the schools policy to always run a DPIA prior to implementing changes to hardware that may have an impact on the security of our information systems.

3. All hardware, computers and mobile devices are to be logged in the asset register which identifies as a minimum, the make, model and location of the item and the named owner (where possible).
4. All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone else, other than in accordance with this policy.
5. Before being commissioned all hardware is to have default passwords changed. This includes ensuring that laptop/desktop computer start up passwords are enabled and that no automatic functions are enabled which trigger action which can create a security vulnerability, such as auto-play functionality.
6. No hardware other than that commissioned or authorised by Seva School is to be used within the organisation for any purpose.
7. Under no circumstances are Pupils, Staff or Visitors permitted to take photographs, videos or audio-visual recordings of any kind without obtaining prior consent in writing from the data subject. This applies to both school owned and personal devices.

Software

1. Only authorized software is permitted on Seva School equipment. Any additional must be approved by Principal.
2. Specific version upgrades are to be approved by Principal.
3. No computer can be used within the business without up to date anti-virus and anti-malware software.
4. Any specific software and/or functions required for work purposes not on the standard list must be approved by Principal.
5. It is the schools policy to always run a DPIA prior to implementing changes to software that may have an impact on the security of our information systems.
6. If you receive an email you suspect to be phishing you must not open this. Please contact IT who will advise how to proceed.
7. If you detect a virus on any IT equipment, this must be reported to IT immediately.

Data storage

1. No external data storage (USB, CD, DVD, mobile device etc) is permitted without encryption and virus scanning. You should also obtain approval from IT before attaching the device to the network.
2. As soon as data has been transferred from an external device to the school's network, this data must be deleted from the device as soon as possible.
3. All electronic data is automatically backed up at the end of every day.
4. Staff should not take any confidential/sensitive information home without the permission of the Principal. If permission is granted then the technical and practical measures taken in the workplace should be taken within your home to maintain the continued security of that information. (i.e., hardcopies kept secure where visitors cannot see it, confidential material should be marked as such)

Email

1. Caution should be taken when sending emails to ensure that information is being sent to the correct person, especially where email addresses auto complete.
2. Staff should be sure to mark all confidential emails as such and circulate the email only to those who need to know this information.
3. Staff should be cautious when opening emails from unknown senders. Do not open attachments or click on links if you are unsure of their safety. Heldesk should be informed of any suspected phishing emails, or suspected viruses etc.
4. Email messages should be written as professionally as a letter. Be concise and direct the email only to the relevant individuals who need to know the information.
5. All staff should remember that emails can be the subject of legal action for example, in breach of contracts, confidentiality, harassment etc against both members of staff and the school. Therefore, please take care with the content of email messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the school in the same way as the contents of letters.
6. Staff must not agree to terms, enter into contractual commitments or make representations by email unless authority has been obtained by Principal.
7. Staff who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material it should NOT be disclosed or forwarded to another member of staff or used in any way. Principal should be informed as soon as possible.
8. Please be mindful that the school reserves the right to access and read any emails sent over the school network and may recover emails, even after they have been deleted.

SOCIAL MEDIA POLICY

This policy applies to all Seva School staff, regardless of their employment status.

Staff are permitted to use Social Media such as Whatsapp, Facebook, linked in etc but we have put in place certain controls to minimise the risks to the school's reputation as well as our confidential and proprietary information.

Personal use of social media is **not** permitted during work hours.

This policy applies to all forms of social media and internet posting. It also applies to the use of social media for both work AND personal purposes both inside and out of working hours.

1. Social Media must not be used to defame or disparage the school, its staff, pupils or parents, stakeholders or third parties. (Current, past or prospective)
2. Staff must not harass, bully or discriminate against other staff, pupils or parents, stakeholders or third parties. (Current, past or prospective) or say anything they may find offensive, including discriminatory comments, insults or obscenity.
3. Staff must not share any personal information about staff, pupils or parents, stakeholders or third parties, (Current, past or prospective)
4. If staff chose to disclose their affiliation with the school as a staff member (current past or perspective), they must also state that their views do not represent those of the schools. Even if staff do so, they must still refrain from posting about any confidential or sensitive school related topics.
5. Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.
6. Staff must not breach any laws or ethical standards
7. Staff must not provide references for other individuals on networking sites as this may be attributed to the school.
8. Staff should not use their work email to sign up to personal social media sites.
9. If staff are contacted for comments about the school for publication anywhere, including any social media outlet, the query must be directed to the Principal and must not be responded to without prior approval.
10. Staff must not use the school's logos, slogans or any intellectual property without prior consent from the Principal.
11. Photos/videos of staff or pupils must not be taken or shared on Social Media without prior consent of the person in the picture or their parent. This includes sharing via messenger platforms such as WhatsApp or Facebook messenger.

If you are unsure if a post is in breach of this policy, please check with the Principal before posting. If you see social media content that is in breach of this policy then please also report it to the Principal.

When posting on the school's social media account you must

1. Get the post approved by Principal
2. Ensure that permission from the child parent has been sought to use photos on social media. This information can be found in Sims.

3. Ensure that there is no identifying information relating to the child. (E.g. their name is not showing on a piece of work)
4. The post must be a positive and relevant post relating to the children, the good work of staff, the school or any other achievements.
5. All photos taken for the purpose of social media/school use on personal devices must be deleted as soon as they are uploaded onto a device belonging to the school.

PASSWORD POLICY

The purpose of this policy is to establish the standard for strong passwords, the protection of those passwords and the frequency of change.

Password Creation

1. All user-level and system-level passwords must conform to the *Password Guidelines*. This is enforced on all systems that we are able to. IT is responsible for administering this.
2. Users must not use the same password for School accounts as for other non-School access (for example, personal ISP account, option trading, benefits, and so on).
3. Where possible, users must not use the same password for various School access needs.
4. User accounts that have system-level privileges must have a unique password from all other accounts held by that user.

There are many actions that staff can take to help ensure password protections and in doing so, helping secure the data that Seva School is responsible for. We ask that all staff take the following steps when dealing with passwords to school apps/systems.

Password Protection

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive,
2. Passwords must not be inserted into email messages or other forms of electronic communication.
3. Do not share School passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
4. If you **must** share a password with a member of the leadership team (when out of the office/sick etc) you must then contact Helpdesk to notify them and to get this password changed ASAP.
5. Any member of staff found to be accessing IT systems using another staff member log in details will be liable to disciplinary action up to and including dismissal for gross misconduct.
6. Do not reveal a password on questionnaires or security forms.
7. Do not hint at the format of a password (for example, "my family name") anywhere.
8. Staff must not leave applications or workstations logged in when leaving your desk/office in order to prevent unauthorised access. If you do leave workstations logged in and this results in a breach – you may be held liable and may result in disciplinary action.
9. Do not write passwords down and store them anywhere in your office/classroom. Do not store passwords in a file on a computer system or mobile devices (phone, tablet,) without encryption.
10. Do not use the "Remember Password" feature of applications (for example, web browsers).
11. Any user suspecting that his/her password may have been compromised must report the incident to the DPO and change all passwords

External contractors and visitors

1. Wi-Fi network passwords should not be given to visitors. If it is given in error, it must be changed immediately.
2. External contractors needing access which requires passwords must sign up to and adhere to all the IT policies/NDA which regular staff sign up to.

PHYSICAL SECURITY POLICY

It is not just cyber security that we need to be aware of in regards to data protection, it is also the physical security of data. Not just to access of computers and networks by allowing visitors into the building but also to paper copies of data stored within the school. The school takes as much care as possible in securing the school.

Paper records and documents containing personal information, sensitive personal information and confidential information must be positioned in a way to avoid them being viewed by others (i.e. not to leave these lying on your desk whilst going to lunch etc) and all such documents must be locked away in a secure cupboard at the end of use. Operations Manager is the only person with access to these locked cupboards, should you need to access any information.

All unattended computers and IT equipment must be locked and only accessible by entering a unique username and password.

CCTV

We have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

- We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
- The named individual who is responsible for the operation of the CCTV system is Operations Manager.
- We regularly review our decision to use a surveillance system
- We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.
- Our system produces clear images which we can easily disclose to authorised third parties. For example when law enforcement bodies (usually the police) require access to investigate a crime.
- We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.
- We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.
- Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted
-

The physical security of the building is of high importance and is reviewed regularly. However, if you find any concerns of liabilities to this security, please report this to the Operations Manager.

Related policies and procedures–

Data Subject Request Procedure

Privacy Statement

Data Breach Procedure

Joiner/Leaver Process

Password Guidelines

Please note: Failure to comply with the above guidelines, and other policies laid out by Seva School may lead to disciplinary action.

I confirm that I have read and understood the above policy -

Employee Name _____

Signature _____

Position _____

Date _____