ST. NICHOLAS SCHOOL

ST. NICHOLAS SCHOOL DATA PROTECTION, DATA SECURITY AND INFORMATION SHARING POLICY

Adapted from the KCC and The Key Model policies for Data Protection

INTRODUCTION (INCLUDING DEFINITION)

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

LEGISLATION AND GUIDANCE

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

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › Name (including initials) › Identification number › Location data › Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

DATA SECURITY

Mobile Data Storage

Under the terms of the UK Data Protection Act 1998, organisations handling personal information about individuals have legal obligations to safeguard that data. According to the ICO, all data kept on electronic media within educational institutions should be kept secure, encrypted and logged in order to keep track of any theft or loss. Where theft or loss does occur and encryption has not been imposed, enforcement action may follow which could be a fine of up to £500,000.

All school laptops and tablets are password protected and, where appropriate, protected with encryption software. All portable storage devices carrying personal data such as USB sticks, portable hard drives, CDs and DVDs should have their personal data encrypted. All staff data files information should be saved directly onto the KLZ OneDrive Cloud storage system as this contains a secure backup. The loss a portable storage device that contains personal or institutional data will constitute a data protection breach.

Any personal information taken offsite in paper form should be carried in a locked box – to promote data security.

Protection

Anti-Virus Protection – This is provided on all networked and laptop / tablet devices using windows as their operating system. Malware protection is also provided by this programme. The school's internet and email traffic is protected by the Kent County Council KPSN broadband system firewall as the primary line of defence – a private network provision with two secure points of presence to the internet, including anti-spam and ('Light Speed') filtering systems. These filters will block the vast majority of sexually or politically inappropriate material and, where appropriate, an incident report will be automatically generated to inform the school of any potentially illegal behaviour.

Password Protection and Encryption plans - All school computers systems are secure with a high standard of password protection. All staff laptops and ipads / tablets are password protected. Each teacher has been provided with an encrypted mobile USB device. Staff laptops are being provided with encryption software as part of the replacement plan.

Email Protection – The school uses the secure KLZ email system. The system contains an electronic moderation filter. If an inappropriate or swear word/term is used within an email, the system automatically

generates an 'incident report' and this is sent directly to Stephen King (Deputy Headteacher). The sender will receive a warning that their email has not been sent and that SLT have been informed. This incident will trigger an interview with the SLT and a behavioural incident form will be created for pupils and a potential disciplinary proceeding may be initiated for members of staff.

Cyber Security Plan

Hardware / Software

The school has a data protection strategy where sensitive data on the admin system is backed up to both the two highly secure sites – the EIS system host and a separate mirror site, on a daily basis. The school has a disaster recovery provision for this data. The school curriculum network is backed up on a nightly / weekly / monthly basis via on-site tapes which are held securely in the school safe. These protocols allow our data to be recovered without payment if there were a ransomware attack.

The school is currently in the process of removing any locally-held sensitive / personal information or curriculum data files from any curriculum device. The plan is in place to migrate all data files from school leadership & management, teacher, HLTA or TA staff machine onto the securely encrypted cloud storage systems (MS OneDrive and / or MS SharePoint) available through the KLZ system.

Staff support and advice

In order to reduce the risk of a phishing attack or trojan horse infection all staff are advised not to open links or attachments in emails, or texts on phones or on their laptops / tablets connected to the schools' system, even if they recognize the sender. Unless an email with an attachment or link was expected, staff are advised to contact the sender and check that they have sent it.

The school staff are aware that when there is (a ransomware) attack the computer will become unstable, unusable or data will start to disappear. They know that if a "splash screen" pops up e.g. demanding a ransom – often for bitcoins – it may come with an offer to have sensitive data returned unencrypted.

It is within the school cyber protection plan that the 'infected' machine is immediately cut off from all networks. The school will then call Action Fraud and the Local Education Officer.

If personal data has been breached / lost the Information Commissioner's Office will be told, via the GDPR in Schools system. All cyberattacks will be communicated to parents and any individual data losses will be reported to the families of the specific pupils concerned.

POLICY INTO PRACTICE

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.

The Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

Governing Body

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer (DPO)

St. Nicholas School currently outsources the official role and responsibilities of The Data Protection Officer (DPO) to "GDPR in Schools" service from Cantium.

Data Protection Lead (DPL)

The Deputy Headteacher is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They are responsible for managing data protection on a day-to-day basis and the reporting / referral / Consultation with the office of the ICO.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

Full details of the DPL's responsibilities are set out in their job description.

Our DPL is Stephen Kingand is contactable via email at: stephen.k@st-nicholas.kent.sch.uk

Headteacher

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

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 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

Every member of staff that holds personal information has to comply with the Act when managing that information. The school will report any breaches of data via the secure SPS / GroupCall "GDPR in Schools" system. This system will also hold evidence of data sharing agreements with our suppliers.

St. Nicholas School is committed to maintaining the eight principles at all times. This means that St. Nicholas School will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared - this is known as a Privacy Notice. The school has prepared and shared / published Privacy Notices for our students and employees.

- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary (the guidelines from the IRMS toolkit [2016] - see appendix D - will be followed).
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act (see appendix E) – this will be provided free of charge.
- Where St. Nicholas School acts as a supplier of training or support services for other organisations, a data sharing agreement will be provided (see appendix F).
- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures
- When sharing personal information outside the organisation and / or internal systems, 'best practice' protocols should always be followed:

If a request has been made of a school staff member to share an electronic data file containing sensitive, confidential or personal information, the following procedure should be followed -

i. The electronic file should be password protected before sharing and sent securely via the KLZ email or Egress Switch systems.
ii. In situations where access to secure systems are not possible, an initial email should be sent to the recipient stating that a file containing personal information will follow. A request for a return email confirming the identity of the recipient and that the email contact is accurate.
iii. A second email should then be sent containing the file of personal information. This message should also include a reminder for the safe, sensitive and confidential management of the personal information, once shared.
iv. In any or every emailing correspondence with a professional from another organisation, the initials of any pupils and / or adults should be used only; this will reduce the risk of a data breach and to ensure data safety / security.
v. St. Nicholas School will operate a screen lock policy – when staff move away from their screen (desktop / laptop / Tablet) or have a colleague approach their work area when sensitive personal data is being used, they will lock the screen to prevent any other people viewing what is on screen. (ICT systems) Staff will set the automatic screen lock time (via display settings) on all staff owned machines to 1 minute.

If a request has been made of a staff member to share information over the telephone -

i. St. Nicholas School staff should ask for the name of the person making the request. The professional (land line) telephone number of the other professional should be taken and, where possible, phone contact should go through a switchboard. A return call will need to be made – to ascertain the identity of the person making the request.
ii. School staff should end the call at this point.
iii. The call should be returned immediately (via the switchboard) and once the other professional has been identified, within their organisation, the verbal information should then be shared.

If a request has been made of a staff member to share information by post -

i. St. Nicholas School staff should share the information required, in a sealed envelope, using initials where appropriate.
ii. If an envelope with a clear window is used, the letter within should be folded in such a way as to hide the personal information.

NB: Staff sharing information should always keep a written record of the reasons for request, thus complying with the HM Government "Seven golden rules for information sharing" (see appendix B).

When making decisions in respect of the handling of personal information, the JAPAN Test should be used to decide if the need to share is Justified, Authorised, Proportional Auditable and Necessary (see appendix C).

DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

LIMITATION, MINIMISATION AND ACCURACY

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

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

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

Where we transfer personal data internationally, we will do so in accordance with data protection law.

SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Due to the Profound Severe and Complex Learning Needs of the Children and Young People at St. Nicholas School, pupils (under 12, aged 13-15 or 16-18 years old) are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other Data Protection Rights of the Individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

BIOMETRIC RECOGNITION SYSTEMS

St. Nicholas School does not use, and has no plans to use, any biometric recognition systems.

CCTV

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.

Any enquiries about the CCTV system should be directed to Stephen King (Deputy Headteacher and DPL).

PHOTOGRAPHS AND VIDEOS

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

We will obtain written consent from parents/carers, and/or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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

See our Child Protection & Acceptable Use of Technology Policies and Privacy Notices for more information on our use of photographs and videos.

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 data protection 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

DATA SECURITY AND STORAGE OF RECORDS

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online Safety and Acceptable Use of Technology policies
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

DISPOSAL OF RECORDS

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

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

PERSONAL DATA BREACHES

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils.

TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

MONITORING

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every **2 years** and shared with the full governing board.

EQUALITY, SAFEGUARDING AND EQUAL OPPORTUNITIES STATEMENT

St Nicholas School, in all policies and procedures, will promote equality of opportunity for students and staff from all social, cultural and economic backgrounds and ensure freedom from discrimination on the basis of membership of any group, including gender, sexual orientation, family circumstances, ethnic or national origin, disability (physical or mental), religious or political beliefs.

St Nicholas School aims to:

- Provide equal opportunity for all
- To foster good relations, and create effective partnership with all sections of the community
- To take no action which discriminates unlawfully in service delivery, commissioning and employment
- To provide an environment free from fear and discrimination, where diversity, respect and dignity are valued.

All aspects of Safeguarding will be embedded into the life of the school and be adhered to and be the responsibility of all staff.

LINKS TO OTHER POLICIES:

CHILD PROTECTION PRIVACY NOTICES STAFF CODE OF CONDUCT (including BRING YOUR OWN DEVICE TO WORK) ACCEPTABLE USE OF TECHNOLOGY ONLINE SAFETY CCTV POLICY FREEDOM OF INFORMATION

STEPHEN KING

REVIEWED TERM 5 2020

RATIFIED BY THE FINANCE AND RESOURCES COMMITTEE AT THE MEETING ON – 11/11/20

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPL/DPO
- The DPL/DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPL/DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPL/DPO will alert the headteacher (and the chair of governors, if appropriate)
- The DPL/DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPL/DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPL/DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPL/DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data

- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPL/DPO must notify the ICO.

- The DPL/DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school cloud storage system.
- Where the ICO must be notified, the DPL/DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPL/DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPL/DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPL/DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPL/DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPL/DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPL/DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above, any decision on whether to contact individuals will be documented by the DPL/DPO.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - Effects

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

Records of all breaches will be stored on the school cloud storage system.

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

Actions to minimise the impact of data breaches

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

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPL/DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL/DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPL/DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPL/DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL/DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen