St. Nicholas School Data Protection and Security Policy

Adapted from the KCC Model policy for Data Protection

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

St. Nicholas School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by St. Nicholas School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

2. The Eight Principles

The Data Protection Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be obtained and processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specific and lawful purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

4. Personal data shall be accurate and where necessary kept up to date.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

9. School staff should follow the KCC and SPS guidance on data protection when requesting, sharing or processing information (see appendix A).

10. Staff working at home or off the school premises, should follow the school Bring Your Own Device To Work Guidelines within the Staff Code of Conduct Policy.

11. 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).

12. 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).

Policy into practice

3. Responsibilities

3.1 St. Nicholas School must:
Manage and process personal data properly
Protect the individuals' right to privacy
Provide an individual with access to all personal data held on them.

3.2 St. Nicholas School (specifically the Headteacher) has a legal responsibility to comply with the Act. St. Nicholas School, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.3 St. Nicholas School is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link :
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

3.4 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.

3.5 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.

13. This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998. With the new EU General Data Protection Regulation (2016) / UK Data Protection Act (2018), 6 things to consider are: Awareness, the legal basis for data processing, a consideration of the information we hold, the right of the people to control their personal information, student rights and how to manage a data breach. In preparation for the new regulations and in the implementation stage of these procedures 12 steps should be taken: Awareness, Information we hold, communicating privacy information, individual's rights, Subject access requests, Lawful basis for processing personal data, Consent, Children, Data Breaches, Data Protection by Design and Data Protection Impact Assessments, Data Protection Officers and the International Dimension (see Appendix G).

    'Children' – to comply with GDPR rules, we will seek the written and / verbal consent of our pupils alongside that of their parents / carers when their personal information is shared – this includes school photographs, trip letters (particularly if a booking / sharing of information is required).

    'International' Dimension – It has been deemed safe to transfer data and have our information backed up onto (cloud) servers hosted off-shore to all the countries of the EEA (EU member states with Lichtenstein, Iceland and Norway). The following countries are also deemed to be adequate data protection rules – Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. In addition, due to the Privacy Shield Network, a finding of partial adequacy has been awarded to the USA and Canada.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact

Schools' Personnel Service,
Tel: 03000 411115
Email: sales @the-sps.co.uk

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.

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 St. Nicholas School and be adhered to and be the responsibility of all staff.

LINKS TO OTHER POLICIES

Safeguarding Health and Safety Online Safety Children in Care Website management Confidentiality Safer Recruitment Volunteer Policy

STEPHEN KING REVIEWED TERM 4 2018 RATIFIED BY THE FULL GOVERNING BODY – 20 JUNE 2018

Appendix A

KCC Guidance on Data Protection - *https://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr*

SPS Guidance on Data Protection – *https://the-sps.co.uk/gdpr*

Appendix B

DFE Seven Golden Rules for Information Sharing Guidelines - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

Appendix C

The JAPAN Test - https://www.kelsi.org.uk/__data/assets/pdf_file/0003/26706/Japan-Test.pdf

Appendix D

IRMS Toolkit - https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

Appendix E

Subject Access Request information - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Subject Access Request Form –

subject-access-request-form.docx

Appendix F

Data Sharing Agreement –

draft data sharing agreement.docx

Appendix G

6 things to consider - https://the-sps.co.uk/pdf_resources/GDPR-in-Schools-Infographic-01.jpg

12 steps to take now - https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf