Data Protection Policy

Last reviewed March 2018

CONTENTS

1. Introduction.

St Nicholas Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. We use this personal information to provide education and for functions associated with the running of our school.

We are registered as a data controller with the Information Commissioner's Office (ICO). Details of the information we hold and the purposes we use it for can be found on the ICO's online Data Protection Register at www.ico.org.uk.

2. Purpose.

This policy is intended to ensure we collect information fairly, use it lawfully and keep it safe in order to comply with the Data Protection Act. This policy applies to any information we hold that relates to identifiable living persons.

All employees, governors, contractors, agents, volunteers and temporary staff must work in accordance with this policy and associated guidance.

3. The Data Protection Principles.

The Data Protection Act contains 8 principles that we must comply with:
1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act;
7. Appropriate policies, procedures and technical measures will be put in place to protect personal information;
8. Personal data shall not be transferred outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

N.B these principles are soon to be replaced with 6 principles within the Draft Data Protection Bill though these have not yet been finalised – the policy will be updated once the Bill has passed into UK law

Unless there is an exemption within the Data Protection Act or other legislation we will do the following in order to comply with the 8 principles:

- explain why we are collecting information and how it will be used at the point we first collect it;
- share information with others only when it is lawful to do so and, whenever possible, with the consent of the person(s) it relates to;

- take extra care in our processing of sensitive personal data which includes information about physical or mental health, religion, race and criminal convictions and proceedings;
- avoid using personal information for any new or substantially changed purposes which were not explained at the point the information was first collected;
- check the quality and the accuracy of the personal information we hold and act quickly to correct details that are found to be inaccurate;
- ensure information is not retained for longer than is necessary;
- ensure that we dispose of information which is no longer required in a safe and secure manner;
- ensure that appropriate safeguards are in place to protect personal information from loss, theft, damage, unauthorised access, unauthorised disclosure or unplanned destruction;
- ensure we have effective procedures to deal with requests from anyone who asks for a copy of the information we hold about them;
- ensure our staff understand our policies and procedures and are provided with appropriate data protection training;
- confirm the identity of persons who contact us before we disclose any personal information to them;
- use appropriate methods to send personal information to third parties in order to ensure it safely reaches the destination;
- investigate any known or suspected information security breaches and take steps to address any risks which are identified;
- Obtain assurances from our suppliers and contractors on their data protection and information security standards before allowing them to access the personal information we hold.

4. Compliance

All staff and governors must work in accordance with this policy and associated guidance. Where a staff member does not comply with our policy there may be extremely serious consequences for the people whose data we hold and for the school. For this reason any failure of a member of staff to comply with the policy will be considered a disciplinary matter which may lead to dismissal.

Staff must remember that they can be prosecuted for breaching the Data Protection Act. Under the Act offences include accessing, obtaining or disclosing information without the data controller's permission and selling, or offering to sell, personal information which has been obtained illegally.

5. Complaints

Complaints and concerns relating to our use of personal information will be taken seriously and will be dealt with in accordance with our complaints policy. Where the complainant is not satisfied with the outcome they may contact the Information Commissioner's Office.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk, telephone 0303 123 1113 (local rate) or 01625 545745 (national rate)

6. Review

This policy will be reviewed at least every 3 years. The review will be undertaken by the Headteacher, or their nominated representative. The guidance which supports this policy will be updated as required and will be communicated to all staff, governors and any other relevant persons with access to personal data held by the school.

7. Contact

If you have any enquires in relation to this policy, please contact the headteacher on 01482444214 or head@st-nicholas.hull.sch.uk or the School Business Manager at admin@st-nicholas,hull.sch.uk who will also act as the contact point for any requests for personal and educational information held by the school.

Appendix 1
Rights of access to information
Any person can request access to their personal information which is held by the school in accordance with the Data Protection Act. This is known as a Subject Access request or SAR. There is a separate process for accessing a pupil's educational record in accordance with the Education (Pupil Information) (England) Regulations 2005, please refer to Appendix 2.

Subject Access Requests
Requests for information must be made in writing (this can include email).

Requests should be addressed to:
headteacher on 01482444214 or head@st-nicholas.hull.sch.uk or the School Business Manager at admin@st-nicholas,hull.sch.uk

Requests will be answered within 30 calendar days however this period will not begin, or may be suspended, until:

- the identity of the applicant has been clearly established (the school reserves the right to request sight of identity documents such as passport or driving licence);
- any clarification the school requests on what information is required is provided by the applicant;

Any individual may request access to information held about them. However, for children this depends upon their capacity to understand and to take informed decisions about themselves (normally from around the age of 12). The Headteacher or their representative will discuss any request involving a child's records with the child and take their views into account when making a decision on whether information should be disclosed.
A child with competency to understand can refuse to allow a request for their records, even if it is made by their parent or guardian. Where the child is not deemed to be competent an individual with parental responsibility or their guardian shall make the decision on behalf of the child.

Complaints
Complaints about Subject Access Requests should be made to the Chairperson of the Governing Body who will decide whether the complaint may be dealt with in accordance with the school's complaints procedure. Complaints that cannot be dealt with through the school's complaints procedure can be considered by the Information Commissioner's Office. We will include details of how to complain where we respond to SARs.

Appendix 2
Education (Pupil Information) (England) Regulations 2005

The Regulations
Under these regulations, the governing body of a school must make a pupil's educational record available for inspection by the parent, free of charge, within 15 school days of the parent's written request for access to that record.

The school must also provide a copy of the record if requested to do so in writing within 15 school days. The school may charge a fee not exceeding the cost of supply.

The meaning of parent is wider than the definition of who has parental responsibility. Parent means a person with parental responsibility or who has care of the child. Therefore, where a child is living with grandparents, the grandparents have a right to see the child's educational record even though they may not have parental responsibility which would allow them, for example, to change the child's name.

Parents have a right to access their child's data under the Pupil Information Regulations and the child cannot prevent this. These Regulations only cover information in the official pupil record.

Exemptions

A school must not communicate anything to the parent which it could not communicate to the pupil under the DPA. Also, the school must be mindful of other individuals' rights under the DPA which might be infringed. For example, where a pupil's parents have divorced and the record contains letters from the pupil's mother, consideration must be given to whether these should be removed from the record before it is shared with the father.

School reports
Every parent is entitled to receive an annual report in respect of his or her child. Parents also have the right to make arrangements to discuss the content of the report with the child's teacher. This right remains even if a child no longer lives with the parent, providing that parent has parental responsibility.

Appendix 3
Information Security and Data Breach Procedure

We must keep our information safe. This is particularly true of the personal information we hold about our pupils, their families, our employees and third parties. However, all our data is important and this procedure applies to any confidential information including details about finance and banking, security arrangements, business matters, contracts and procurement processes.

It is important that our employees understand what to do in the event that something goes wrong and our information is put at risk. All employees must report any known or possible incidents where information or the files/systems containing them has:

- been lost or stolen;
- been sent or disclosed to another party in error;
- been sent without adequate security protection or safeguards;
- been accessed by someone who does not have permission to do so (including our staff and pupils);
- become unavailable for an extended period due to problems with our computers or IT network;
- become unavailable due to fire, flood or other problems with our buildings;
- been the target of any attempt to 'hack' our computer systems, including malicious emails;
- been the target of any attempt to gain access to information by deception (this is known as 'blagging');
- been processed in any way that breaches the Data Protection Policy or other policies governing *how* ***St Nicholas Primary School*** manages its information.

Incident Response

Where somebody may be at immediate risk of harm a senior member of school staff must be informed **immediately** and all reasonable steps must be taken to warn the individual(s) without delay. In such circumstances consideration should also be given to contacting the Police.

In the event or any known or suspected breach of information security the following steps must be taken –

1. The staff member who identifies the breach must notify the School Business Manager, Deputy Head Teacher or Head Teacher immediately. If the incident is discovered outside St Nicholas Primary School's opening hours it must be reported as soon as it reopens. If an incident is considered particularly serious, (for example if someone may be at risk of physical harm or lots of records have been compromised) the incident should be reported immediately by contacting <insert out of hours contact details>.

2. The staff member handling the incident must -

a. Establish whether information is still being put at risk. If so steps must be taken to secure it immediately - for example contact the IT Supplier to shut down a compromised system or arrange for a security company to board up a door or window.
b. Decide if, when and how any individuals affected by the incident will be notified and what advice they should be provided with.
c. Where possible, and safe to do so, attempt to recover lost or stolen information or equipment.
d. Report any criminal activity and lost or stolen property to the Police.
e. Have school staff immediately change any passwords or access codes that may have been compromised and warn them if they might expect phishing emails or other malware to be sent to them.
f. Notify the Head Teacher and Chair of the Local Governing Body in a timely fashion, they should be informed quickly about more serious incidents.
g. Where the information could aid fraudulent activity, consider the need to notify banks or companies and organisations we work with.
h. Take any steps to recover data from back-ups or copies held elsewhere.
i. Consider any possible impact on the running of the St Nicholas Primary School, take steps to inform any affected parties and mitigate the impact upon them.
j. If the incident may be newsworthy, consider the need to take media relations advice, for example from the Council's Media Team.
k. Where very sensitive personal data, or large volumes of less sensitive personal data, has been compromised it may be appropriate to report the breach to the Information Commissioner's Office (ICO). From May 2018 serious incidents must be reported within 72 hours. Guidance is available on the ico.org.uk website or on the ICO telephone helpline.
l. Keep records that will demonstrate what has happened and assist an investigation into what went wrong.

The Council's Information Governance Team will help with response to data breach and information security incidents. They can be contacted for advice on (01482) 613295 or 613378, or information@hullcc.gov.uk

Staff should note that it is **not** the policy to of **St Nicholas Primary School** to pursue serious disciplinary measures against staff who make genuine human errors but any failure to report or attempt to hide an information security incident will be dealt with extremely seriously.

Investigation

Once the initial response to the incident has taken place it is important that the full circumstances are properly investigated. This should be done promptly to ensure that any ongoing risks can be identified and addressed.

The investigation should be undertaken by a staff member nominated by the Head Teacher; this can be the person who dealt with the initial incident response.

The investigation should include consideration of the following –

1. What data was compromised, including numbers of records and their sensitivity?
2. What happened, where appropriate including a chronology of events?
3. Review existing safeguards and procedures, how effective they were and any additional measures that could be put in place.
4. Known or potential adverse impacts on data subjects and any advice or support that should be provided to them.
5. Any breaches of policy or procedure and how these should be addressed.
6. Any HR or disciplinary action that may be necessary.
7. Costs and any likely financial implications for St Nicholas Primary School.
8. Potential for any ongoing illegal or unauthorised use of the data.
9. Consideration of any issues with partners or suppliers.
10. Regulatory issues and whether the matter was reported to the ICO.
11. Any offence under Section 55 of the DPA (knowingly or recklessly obtaining or disclosing personal data) that may need to be reported to ICO or the Police.
12. Any warnings or issues that should be shared with local partners such as other schools and academies or the Council.

Review

The staff member nominated to undertake the investigation should present their report to the Head Teacher. Where further action is recommended it should be agreed who will be responsible and set timescales for any actions.

The Head Teacher will provide a summary of incidents to the Chair of the Local Governing Body once each school year.