St Thomas Centre Nursery School

E Safety Policy

To include policy for use of Social networking sites
Data protection

Article 17 (Access to information; mass media): Children have the right to get information that is important to their health and well-being. Governments should encourage mass media – radio, television, newspapers and Internet content sources – to provide information that children can understand and to not promote materials that could harm children. Mass media should particularly be encouraged to supply information in languages that minority and indigenous children can understand. Children should also have access to children's books.

At St Thomas Centre Nursery we follow the policies and procedures from Birmingham City Council and Birmingham Safeguarding Children Board (BSCB) which includes the government's PREVENT Strategy.

Name	
Role	
Date	
Signature	
Next review	

BIRMINGHAM CITY COUNCIL

E-SAFETY POLICY FOR SCHOOLS

1. Introduction

1.1 The governing body of St Thomas Centre Nursery has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was adopted by the governing body on October 21st 2014 and will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the head teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The governing body expects the head teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing body

3.1 The governing body will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in e-safety training if they use information and communication technology in their capacity as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head teacher

3.3 The head teacher is responsible for ensuring that

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- the governing body is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- the school has a designated senior person to co-ordinate e-safety and that this person has adequate support from, and provides support to, other employees, particularly the designated senior person for safeguarding;
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with training in e-safety relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be;
- pupils are taught e-safety as an essential part of the curriculum;
- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the senior leadership team;

- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the head teacher commensurate with their salary grade and job descriptions;
  - participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
  - using information and communication technology in accordance with this policy and the training provided;
  - reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

  - participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
  - use information and communication technology in accordance with this policy and the training provided;
  - report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;

- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

4.3 Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

5. Education and training

5.1 Education and training in e-safety will be given high priority across the school.

5.2 The education of pupils in e-safety is an essential part of the school's e-safety provision and will be included in all parts of the curriculum.

5.3 The school will offer education and information to parents, carers and community users of the school about e-safety.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of information.

7. Technical aspects of e-safety

7.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably

possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

7.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

8. Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

POLICY FOR THE USE OF SOCIAL NETWORKING SITES

St Thomas Centre Nursery respects an employee's right to a private life. However, the Centre must also ensure that confidentiality and its reputation are protected. It therefore requires employees using social networking websites to:

- Refrain from identifying themselves as working at the Centre.
- Ensure that they do not conduct themselves in a way that is detrimental to the Centre e.g. personal photographs showing inappropriate behaviour such as drunk and disorderly, sexually explicit images, making reference to illegal actions etc.
- Take care not to allow their interaction on these websites to damage working relationships between members of staff or clients of the Centre i.e. 'Cyber Bullying' referring in a derogatory way to colleagues, parents or children.
- For employee's own protection and to ensure they comply with the guidelines above, they should ensure privacy settings are such that colleagues and parents (past and present) are not able to view personal content.
- The Centre asks that employees do not accept current parents/carers/service users as friends.
- Social networking sites and web-blogs must not be accessed during working hours.

Employees should ensure that they do not breach the law or breach St Thomas Centre Nursery School Code of Conduct, defame the Centre or its suppliers, or employees, disclose personal data or information about any individual that could breach the Data Protection Act 1998, include material that is sexist, racist or otherwise actionable or bring the Centre into disrepute.

The Centre does not support employees to write about their work and are asked to refrain from doing so on these sites. If individuals choose to do so then they should follow the rules above. Employees who have a web-blog should not disclose the name of the Centre on it or allow it to be identified by any details at all.

Employees are able to take their own guidance on this matter.

The option available to the Centre is to take disciplinary action (see Disciplinary Policy) if an employee's action is to the detriment of the Centre or damages its reputation.

St Thomas Centre Nursery School Data Protection Policy

1 The school will comply with:
- 1.1 The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- 1.2 Birmingham City Council's Children, Young People and Families Directorate advice and guidance.
- 1.3 Information and guidance displayed on the Information Commissioner's website.

2 This policy should be used in conjunction with the school's ***Internet Usage Policy***.

3 Data Gathering
- 3.1 All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- 3.2 Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

4 Data Storage
- 4.1 Personal data will be stored in a secure and safe manner.
- 4.2 Electronic data will be protected by standard password and firewall systems operated by the school.
- 4.3 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- 4.4 Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- 4.5 Particular attention will be paid to the need for security of sensitive personal data.

5 Data Checking
- 5.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- 5.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

6 Data Disclosures
- 6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

6.2 When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

6.4 Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

6.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

6.6 Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

6.7 Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.

6.8 A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

7 Subject Access Requests

7.1 If the school receives a written request from a data subject to see any or all personal data which the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.

7.2 Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

8. Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data