**E-Safety Policy – incorporating Data Protection August 2015**

The Governors of St Edmund's Nursery School & Children's Centre prioritises the safety of everyone using our services including children, families and staff. Several policies consider the different aspects of safety and this e-safety policy should be read in conjunction with

- Child Safety Policy
- Child Protection Policy (including Safeguarding)
- ICT and Communications Policy
- Bradford Council's "Managing Investigations" Toolkit (copy attached)
- Missing Child Policy
- Site Health, Safety and Security
- Inclusion Policy
- CCTV Policy
- Lone working/Outreach Policy
- Outings and Educational Visits Policy
- Recruitment, Induction and Retention Policy
- Student Policy
- Guidance for Safer Working Practice
- Staff Handbook

The Governors appreciate that electronic communications are an essential element in 21st century life for education, business and social interaction. The Governors also support the children in using ICT as part of their learning experience across all curricular areas and believe that used correctly ICT will not only raise standards, but it will support teachers' professional work and it will enhance the school's management information and business administration systems.

## Aims

- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To support children in using ICT resources appropriately.
- To manage the use and storage of electronically stored materials including photographs and videos in order to safeguard children from potential risks.
- To provide clear guidance in the use of mobile telephones and cameras.
- To have the appropriate mechanisms to intervene and support any incident where appropriate.

## Guidance on use of the Internet

### Authorising Internet access

Prior to commencing employment at St Edmund's Nursery School & Children's Centre staff must read and sign the 'Policy on School/Centre ICT and Communications Systems". All staff have an equal responsibility for ensuring safe use of the internet and should they discover any potentially unsafe or inappropriate material, they are to hide the content from view. For example, the window will be minimised and/or the monitor (not computer) will be turned off. This should then be reported to a member of the Senior Leadership Team.

Inappropriate use of the internet will be treated as an act of gross misconduct - if an allegation of misuse is reported to a senior member of staff they will undertake the following procedures in conjunction with the Authority's document "Managing Investigations". As each staff member logs onto the computer they must accept the ICT terms and conditions before they can continue their usage.

**Complaints procedures**

- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be referred to the named person(s) and dealt with in accordance to school/centre's Child Protection procedures
- As with other safeguarding issues, there may be occasions when the police must be contacted.

**Cyberbullying**

*Legal definition (http://en.wikipedia.org)*

Cyberbullying is defined in legal glossaries as

- Actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm another or others.
- Use of communication technologies for the intention of harming another person
- Use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or text messaging with the intention of harming another person.

The Governors/Headteacher will immediately investigate any instances of cyberbullying.

**Information system security**

In partnership with the school/centre's IT support, the Governors will review IT security regularly - virus protection (Sophos) is updated regularly by the authority and filtering software is also used (Surf Protect and Policy Central). All staff have log-on passwords and these must remain confidential – it is recommended that staff routinely change their passwords to protect against irregular use.

**E-mail Communications**

All official online communications must occur through secure filtered email accounts. Web-based commercial email services are not to be considered secure. All ICT users are to be advised not to open emails where they do not know the sender or where the format looks suspicious. Staff are not allowed to log on to personal e-mail accounts whilst at work.

If there is no alternative to using e-mail to send personal or sensitive data then it is best to send it as an encrypted attachment. This may mean writing the e-mail as a Word document, encrypting the document and sending this as an e-mail attachment. Word files can be encrypted using tools such as WinZip or 7Zip. If sending encrypted attachments always use an alternative method, such as text or telephone call, to send the password for the encrypted file. This way, if the e-mail is intercepted, the person who intercepts the e-mail does not have access to the password. This also protects the e-mail if it is accidentaly sent to the wrong person.

**School/Centre Web Site**

Whilst the Governors aim to make the school/centre website accessible to all, no personal information will be displayed.

Contact details on the website will be:
- The school/centre address
- The "office" e-mail address
- The school/centre telephone number

The school/centre website will not publish:
- Staff or pupils contact details
- Pictures of children without the written consent of the parent/carer
- The names of any pupils who are shown

Permission for the use of children's images is sought during the home visit process prior to the child's admission (see attached Registration form).

**Social Networking**

It is to be recognised that staff are likely to use social networking sites in their recreational time on their own personal computers. It must be ensured that the use of such sites will not compromise professional integrity or bring the school/centre into disrepute. The adding of children and young people, parents and carers as 'friends' to a social networking site is prohibited.

**Support for children**

**Assessing risks**

The school/centre will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the nursery network. The school cannot accept liability for any material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

**Advice for parents at home**

At St Edmund's we try to raise awareness of issues that may relate to children's use of electronic information and offer the following guidance on our web site.

**E-Safety – keeping children safe online**

The Internet offers a means to share and communicate in a variety of different ways. St Edmund's supports children to use computers as part of their learning experience; we talk to children about Internet safety, and make sure that the sites children access when they are in the school/centre are safe.

Parents and carers need to take equal care at home:
- Keep the computer/laptop in a communal area such as a family room where you can keep an eye on what your child is accessing on the internet.
- Use an appropriate filtering system to minimise opportunities to access unsuitable material – if you are in doubt about the filtering system you have in place you can contact your service provider to discuss how you can limit access to inappropriate internet sites e.g. pornography or gambling websites.

Get your child into good habits early – make it a rule that:

- Your child always checks with an adult before they use the Internet or email.
- Your child only talks online to people they know.
- Your child never tells anyone how old they are, where they live, or arranges to meet someone they don't know.
- Your child only uses the Internet to look for things they know they are allowed to look at. If they're not sure they should check with an adult before they search.
- Your child is polite when they talk or post things on the Internet and doesn't say things that will upset people.

Your child should also know that if they see anything that worries or upsets them on the Internet or in an email that they ask an adult for help straight away. More information is available at Get Safe Online.
Other useful links:
Childnet
CEOP Thinkuknow website
UK Safer Internet Centre

**Management of data**

The Data Protection Act 1998 (the Act) applies to anyone who handles or has access to information concerning individuals. Everyone in our setting has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (defined as information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

The quantity and variety of data held on pupils, families and on staff is always expanding. Whilst this data can be very useful in improving services, data could be mishandled, stolen or misused. The Governors are aware that the security of personal data is always paramount and ensure that portable media, such as memory sticks, can only be used if they are password protected.

The Act promotes openness in the use of personal information ensuring that every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. St Edmund's Nursery School & Children's Centre is registered with the Commission and its Registration number is Z9752909.

Parents are given a copy of the school/centre Privacy Notice as part of the Home Visit pack (copy attached).

## Mobile Telephones & Cameras

### Photographs and video

General signed consent to take photographs or record images of children will be requested from the parent or carer on of enrolment their child (see attached Registration Form). The purpose for taking any images is to be clearly explained and agreed. The Registration Form also allows for parents to consent to their child's image being used in publicity materials (eg web site)

It should be recognised that some children will be more vulnerable than others, for example children with disabilities, children in care, those with a child protection or child in need plan. For a range of reasons, such children's security may be compromised more than others, and therefore extra precautions must be considered in such circumstances.

Staff must ensure that if they transport photographs out of the building, for example to work on children's records at home, that they use an encrypted data pen.

### Parents taking photos

Parents are requested not to take photographs within the school/centre, either with a camera or mobile telephone. There are circumstances such as school/centre visits where this may be allowed but all parents are made aware that their child can be excluded from this and not allowed to be photographed/videoed when they complete the Registration Form

### Mobile Telephones

Mobile phones will cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. All service users, including parents, carers, visitors and contractors are advised that their mobile phones are not to be used within the children's areas.

Staff use of their personal mobile telephones should be confined to break periods ONLY. Designated areas for use of mobiles are Staffroom and Admin Offices areas. It will be considered a GROSS MISCONDUCT offence to use mobile telephones in any other area. Under no circumstances should mobile telephones be used to take photographs of children.

Staff should be aware that it is illegal to make or take a phone call, text or use the enhanced functions of a mobile phone whilst driving. The governors also feel that this should also to apply to the use of hands free and wireless connections, which are to be considered a distraction rather than a safer alternative.

## Training

- As part of the policy review process staff and governors will consider the E-safety Programme on a rolling programme.
- Staff are given updates on internet security (eg "How to lock down your Facebook" – see attached)
- The Leadership Team has received training in "Safeguarding: Safe use of Social Media"
- Administrative staff are trained in line with Council Policy by the IT training section (eg management of pupil/staff data)

## Promotion of the Policy

The Governors will promote this policy as part of the Staff Induction process. Staff should be aware that network and Internet traffic can be monitored and traced to the individual user and that discretion and professional conduct is essential. The monitoring of Internet use is a sensitive matter and will only be undertaken by the Headteacher or Business Manager.