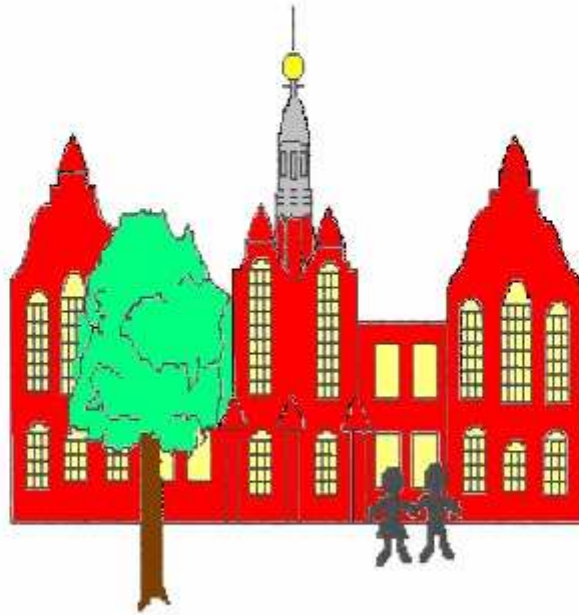


Stepney Primary School



A Small School With Great Expectations

E-safety Policy

At Stepney raising the achievement and basic skills of pupils and ensuring that they reach their full potential is the responsibility of all staff.

1. BACKGROUND

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- access to illegal, harmful or inappropriate images or other content;
- unauthorised access to / loss of / sharing of personal information;
- the risk of being subject to grooming by those with whom they make contact on the internet;
- the sharing / distribution of personal images without an individual's consent or knowledge;
- inappropriate communication / contact with others, including strangers;
- cyber-bullying;
- access to unsuitable video / internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. RESPONSIBLE USE OF THE INTERNET

As part of pupils' curriculum enhancement and the development of ICT skills, *Stepney Primary School provides supervised access to the Internet including e-mail.*

Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the Council/School cannot be held responsible for the nature or content of materials accessed through the Internet. The Council/School will not be liable under any circumstances for any damages arising from your child's use of the internet facilities.

Should you wish to discuss any aspect of Internet use please telephone the Head teacher or the ICT Co-ordinator to arrange an appointment on tel: 343690.

4. RULES AND RESPONSIBLE INTERNET USE

4.1 General

Pupils are responsible for good behaviour on the internet just as they are in a classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards.

Staff are permitted to use ICT and the internet for their own purposes but have to adhere to the policies and guidance that the governing body has adopted from Kingston Upon Hull City Council, namely: 'Policy on the use of Information Technology Procedure for Managers'; 'Policy on the use of Information Technology Procedure for Managers' and 'Guidance on the Use of Information Technology' (Hull City Council Human Resources Implementation Date: 4th November 2003 Revised: September 2007). These are available in the staffroom, or from the school office.

Specifically, staff must not use ICT/Internet for their own personal (non-school related) business at times when they are responsible for and/or in the company of pupils.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear responsibility for such guidance just as they do with sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted in school:

- usage without staff oversight;
- sending or displaying offensive messages or pictures;
- using obscene language;
- harassing, insulting or attacking others;
- damaging computers, computer systems or computer networks;
- violating copyright laws;
- using others passwords;
- trespassing in others folders, work or files;
- intentionally wasting limited resources;
- sending images or personal information of children via the internet unless permission has been granted by parent/carer.

Disciplinary Action:

Staff must note that misuse of the internet may result in disciplinary action that could be addressed through other relevant school policies.

4.2 Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

4.3 Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the schools Staff Information Handbook which refers to acceptable use;
- they report any suspected misuse or problem to the ICT Co-ordinator /Head teacher;
- digital communications with pupils (email) should be on a professional level;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the school e-safety and acceptable use policy;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-safety issues related to the use of mobile phones, computers, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.4 The Child Protection Co-ordinator Miss J Atkinson is aware of e-safety issues and the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

4.5 The ICT/e-safety co-ordinator, Mr P Browning should ensure that:

- update training on e-safety should be delivered to staff when required;
- training content changes in each of these sessions to reflect advances in technology;
- at least him or one member of staff is an e-safety certified professional (e.g. CEOP, EPICT etc);
- surveys are undertaken of staff, pupils and parents;
- the e-safety policy is regularly reviewed;
- that pupils can recall rules;
- that there is evidence about e-safety awareness;
- pupils are made aware of e-safety in assemblies and in programmes across all age groups.

4.6 Pupils should:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school.

5. POLICY STATEMENTS

5.1 Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- key e-safety messages should be reinforced as part of a the curriculum;
- pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- rules for use of ICT systems will be posted in all rooms;
- staff should act as good role models in their use of ICT, the internet and mobile devices.

5.2 Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

5.3 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

5.4 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- users should not expect that files stored on servers or disks would always be private;
- only transferred to others with adequate protection.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- transfer data using encryption and secure password protected devices.

When using communication technologies the school considers the following as good practice:

- the official school email service may be regarded as safe and secure and is monitored;
- users need to be aware that email communications may be monitored;
- users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email;
- any digital communication between staff and pupils or parents / carers (email, chat, social networking etc) must be professional in tone and content;

- staff and pupils will be reminded of the dangers of inappropriate use of social networking sites, including publication of images linked to school or staff social events;
- pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

NB:

The school has an email website at www.stepney.hull.sch.uk.

- From July 2009 this is the only official site produced by Stepney Primary School. We are not responsible for and do not endorse any other sites linked to the school. These include social networking sites.
- From Summer 2011, the school started to use the DB learning platform. Pupils and staff may correspond via an email system on this platform. Pupils and staff have been reminded of the e-safety procedures listed above. The platform has a number of e-safety features, which have been explained to staff and pupils. These include a 'whistle blowing' facility on the emails, whereby children can signal any unwelcome emails to the headteacher and/or administrator. Chat rooms on the site can only work as long as the class teacher is logged on; Surveys and quizzes can only be made available to the rest of the school population when the teacher has vetted and then 'published' them.
- From Autumn 2013, the school started to update information onto the kidblog site. This has become a much-used site by staff and pupils. Similar to other sites used by the school, the head teacher retains administrator rights over this and is able to vet every post or comment that is uploaded onto this site, whether by Stepney staff/pupils or any other bodies.
- The head teacher follows up complaints made by pupils or staff.

6.0 PUBLIC SECTOR EQUALITY DUTY

Please note: When we updated policies from April 2012 onwards, we referred to the requirements of the PSED, which state that as part of their statutory duties, schools need to comply with this by 6th April 2012.

The Equality Act 2010 replaced and unified all existing equality legislation such as the Race Relations Act, Disability Discrimination Act and Sex Discrimination Act. It aims to ensure that people have equality of opportunity in accessing and experiencing public services. Schools when carrying out their day to day work should have regard to the following:

- eliminating discrimination;
- advancing equality of opportunity and
- foster good relations across all characteristics

Schools cannot unlawfully discriminate against pupils because of their disability, gender, race, religion or belief, sex and sexual orientation. Protection is now extended to pupils who are pregnant or undergoing gender reassignment. This means it is now unlawful to discriminate against a transgender pupil or a pupil who is pregnant or recently had a baby.

When this policy was reviewed and updated it was checked that it still made reference to this duty. The author/s of this document and the Policy Committee of the Governing Body, which checks all policies before publication, considered this policy in the light of these requirements to ensure that Stepney Primary School adheres to these statutory regulations.

7.0 PERSON RESPONSIBLE

This was originally updated by Mrs M Codd to replace our 'Use of the Internet Policy' and was adopted by the governor's Sub-Committee Curriculum meeting in Spring 2011.

Updated Spring 2017
Mr P Browning
To be reviewed Spring 2018