Cottesbrooke Infant & Nursery School

E-Safety Policy

Our Vision

Cottesbrooke Infant & Nursery School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Cottesbrooke Infant & Nursery School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and children while on the school premises.

Related Documents:

Acceptable Use of the Internet Policy

Safeguarding Policy

Data Protection Policy

Behaviour Policy

Anti-bullying Policy

ICT Policy

Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.cottesbrooke-inf.bham.sch.uk
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-Safety information in all areas where computers/ mobile devices are used
- Provide e-Safety information to parents.

Roles and Responsibilities

The Head Teacher and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school. The role of e-Safety co-ordinator has been allocated to Ish Shar, ICT Operations Technician and in his absence Will Loughlin, the Head Teacher. They are the central point of contact for all e-Safety issues and will be responsible for day to day management.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety co-ordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Additional roles and responsibilities are discussed in the school's Acceptable Use of the Internet Policy. These will be communicated to the relevant groups at appropriate times.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the e-Safety log for audit purposes.
- Requests for changes to the filtering will be directed to the e-Safety co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the e-Safety log for audit purposes
- The school uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
- Pupils use is monitored by Staff
- Staff use is monitored by the Head Teacher and the ICT Operations Technician

- All staff are issued with their own username and password for network access. Trainee teachers and long term supply staff are issued with temporary IDs and the details recorded. Other students/ visitors will be issued with a temporary username/ password on request
- Foundation stage pupils use year group logon IDs for their network access

- Key stage one pupils have their own username.

Mobile / emerging technologies

- Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policy applies to this equipment at all times.
- Where staff at the school are provided with an iPad or other tablet computer they are for educational use and their own professional development. All staff understand that the Acceptable Use Policy applies to this equipment at all times.
- A school mobile phone is available to staff that may be contacted by parents
- A school mobile phone is issued to the Deputy Head Teacher that may be contacted by staff and college students.
- The school subscribes to Group Call, a system which allows the school to contact parents via text message.
- To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones in line with guidance in the staff Handbook and under usual circumstances not in front of the children
- The Educations and Inspections Act 2006 grants the Head Teacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head Teacher will exercise this right at their discretion
- Pictures / videos of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

- All staff are given a school e-mail address and understand that this must be used for all professional communication. Staff must not use their own personal email addresses for school business.
- Key stage one pupils have access to class based e-mail accounts that are monitored by the class teacher
- All pupils are given a school e-mail address that can be used for educational purposes
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the Acceptable Use policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible

Published content

The Head Teacher takes responsibility for content published to the school web site but delegates general editorial responsibility to Judith White the Office Manager. Staff are responsible for the editorial control of work provided for publication.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office
- The school does not publish any contact details for the pupils

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in line with Becta guidance and will not identify any individual pupil by name
- Students' full names will not be published outside the school environment

In the future, as the technology is adopted:

- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Pupils understand that they must have their teachers permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the pupils

Social Networking and online communication

The school currently does not allow access to social networking sites.

Guidance is provided to the school community on how to use these sites safely and appropriately. This includes

- Being selective about publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites as the need arises.

Any external matters evolving from a social networking site will not be supported by the school.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity

E-safety training

The school has a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance based on the needs of the staff.

- There is an induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by curriculum co-ordinators and disseminated through curriculum meetings / staff meetings / training sessions
- E-Safety is embedded throughout the school curriculum and highlighted by each year group as required. It is specifically taught in Year 2
- Pupils in Year 2 are taught how to validate the accuracy of information found on the internet
- The Head Teacher, DSL and ICT Operations Technician are available to provide appropriate advice and guidance to parents when required through drop in sessions and school publications.
- The school will work to educate parents regarding e-safety and film and video game classifications through workshops and information on the school website.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998

Data is stored on the school systems and transferred in accordance with the Birmingham Education Service advice and guidelines.

All staff are provided with an encrypted data storage device for the transfer of identifiable data.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office on request.

Equal Opportunities

Regardless of age, disability, gender, race, religion or belief, or sexual orientation, e-safety is an issue which applies to all staff, children and visitors.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head Teacher
- Breaches of this policy by staff will be investigated by the Head Teacher. Action will be taken under the school's Safeguarding Policy and/or Disciplinary Policy where a breach of professional conduct is identified. Where appropriate incidents will either be referred to the LADO team or will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- Pupil policy breaches relating to radicalisation, bullying, drugs misuse, abuse and suicide must be reported to the Senior Designated Lead/ SPOC and action taken in line with school anti-bullying and safeguarding policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct inline with school Behaviour Policy. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor pupil offenses, such as being off-task visiting games or other websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head Teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

Date: January 2011

Reviewed and updated: May 2015