Online Safety Guidance

ENFIELD
LEARNING TRUST
BE INCLUDED

Version and Date		Action/Notes	Date Written	Date to be Reviewed
3.0	02.09.19	Approved by CEO	Reviewed July for Sept 19	1 Year – July 2020

This guidance should be read in conjunction with the ESCB online strategy for schools and education settings - December 2013.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high- quality, but safe Internet access as part of their learning experience.

Through the use of the Internet and mobile devises, we ensure that the school equalities policy, safeguarding procedures and curriculum prevent all forms of extremism and radicalisation.

Rationale

Online Safety reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

It encompasses not only internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the benefits of these technologies in educating children and young people, but also the risks and responsibilities of using them. It provides safeguards and raises awareness to enable users to control their online experiences.

Aims

This guidance identifies the measures in place in our Trust:

- to protect children from undesirable content on the internet
- to protect them from undesirable contacts over the internet
- to prevent unacceptable use of the internet by children or adults
- to address issues of copyright for materials published on the internet

Roles and Responsibilities

Online Safety is a whole-school responsibility dependent on all stakeholders, e.g. staff, The Local Governing Board, parents, and advisors. It is also up to the pupils themselves to ensure they act responsibly when using the internet and other forms of communication. The major consideration in creating a safe e-learning environment is internet-safety education, which occurs in the classroom itself and is initiated by the teacher or teaching assistant. Whilst the Headteacher has overall responsibility for online safety issues, a senior manager has delegated responsibility as the Online Safety Leader.

Education

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Permission to Use the Internet

The internet can provide pupils and all stakeholders with opportunities to experience and access a wide range of activities, resources and information to support and enhance the learning and teaching across the whole school curriculum. All pupils will be expected to access the internet unless parents indicate otherwise at the time their child is admitted to school.

In your admission pack you will be required to sign the parental consent form to acknowledge the school policies and procedures.

Online Safety documents will be published on the website for everyone to access.

Accessing and Using the Internet

Pupils use individual logins whenever possible. Pupils will be taught to use the internet safely and responsibly as an integral part of e- learning across the curriculum, supported by the school's Online Safety policy. Pupils will be taught how to keep themselves safe whilst online at home as well as at school.

Content

Unintentional Exposure of Children to Inappropriate Content

It is the Enfield Learning Trusts intention that all reasonable steps will be taken to prevent exposure of children to undesirable materials and inappropriate content on the internet. However, it is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search produces unexpected results.

To protect children from such occurrences, the school has adopted the following position.

In-school protection by:

- adult supervision of pupils' internet activity, with access or searching on the internet **only allowed** with a suitable adult present in the room;
- the "caching" of internet sites by staff, whenever possible in advance, to verify the site and its content;
- children being taught to become critical and discriminating users of materials they find online, through questioning the source and reliability of any content they access, and by being aware

of ways to minimise risks.

Intentional Access to Undesirable Content by Children

Children should never intentionally seek offensive material on the internet. Any such incident will be treated as a disciplinary matter, and the parents will be informed.

In the event of children gaining access to undesirable materials, the following steps will be taken:

- the teacher will report the incident to the Online Safety Leader and Headteacher;
- the incident will be recorded in a central log located in the school, and a Serious Incident Form completed. The school will reliably report the frequency and nature of incidents to any appropriate party.
- parents will be notified at the discretion of the Headteacher and according to the degree of seriousness of the incident. For example, exposure to materials that include common profanities might not be reported to parents, but exposure to materials that include pornographic images would be reported;
- the Headteacher will regularly notify The Local Governing Board of any incidents involving inappropriate or unacceptable use of school internet/ICT facilities as part of the Headteacher's Report.

Intentional Access to Undesirable Content by Adults

Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Local Governing Board will be advised.

Risks Associated with Contact

The internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communication skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may become involved in inappropriate antisocial or illegal behaviour whilst using new technologies e.g., cyber bullying, identity theft, or arranging to meet people they have met online.

Whilst children will, at times, use e-mail as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their learning.

Receiving and Sending of E-Mails by Children

It is recognised that e-mail messages received by children can contain language or content that is unacceptable and that some people may try to use e-mail to identify and contact children for unacceptable reasons. If any member of staff believes that a child has been targeted with e-mail messages by parties with criminal intent, the messages will be retained. The incident will be recorded and the Local Governing Board, and the child's parents, will be informed. Advice will also be taken regarding possible further steps.

To avoid these potential issues the Trust has adopted the following practices:

- the use of the accredited e-mail service which includes the filtering of all incoming and outgoing messages for inappropriate content and spam;
- pupils only read e-mail messages when a member of staff is present, or the messages have been previewed by the teacher;
- children are taught not to open or respond to e-mails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken;
- steps are taken to verify the identity of any school or person seeking to establish regular e-mail contact with this school;
- pupils save their e-mails/messages to 'Draft' for the teacher or teaching assistant to approve before being sent;
- to prevent children revealing their identity within e-mail messages, only the child's forename is revealed, and this is only when appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school web site or learning platform particularly in association with photographs. This includes in file names or in the <ALT> tag. Full names will not be published in any videos/ DVDs produced by the school.
- Written permission from parents will be obtained before photographs of pupils are published on the school web site or learning platform. No children who the SENCo feel are at particular risk will have their images shown.
- Pupil's work can only be published with the permission of the pupil and parents.
- If parents wish to take photos/video of school events e. g assemblies, concerts please be aware these must be for your own private/personal use and images must not be used inappropriately
- Please do not obscure the view of others when taking photos

The use of social networking and online media

The Enfield Learning Trust asks its whole community to promote the 3 commons approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is online-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the Trust and can potentially lower the Trust/ school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, pupil or parent is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

Any breach of serious cases this may lead to disciplinary action under the school's disciplinary policy/ code of conduct. Serious breaches, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Use of social networking by staff in a personal capacity
It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the trust/ school, pupils, parents or colleagues including members of the Trust Board or Local Governing Board.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.

- Inappropriate use by staff should be referred to the CEO/ Headteacher in the first instance and may lead to disciplinary action.

Other Use of the Internet and E-Mail Facilities

The Trust internet/e-mail facilities should be used only for educational purposes during teaching and learning time. If a member of staff chooses to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, they do so at their own risk. Staff who have their own children at The Enfield Learning Trust, or whose children have social contact with Enfield Learning Trust pupils, must be extra vigilant when accessing social network sites.

Staff must be aware of and make sure they understand the dangers of using social networking sites. Staff using these sites must ensure they have high security settings and must not disclose Trust information

Communication with children through technology

Adults or volunteers who work with children should be mindful of how they use social media and the potential for others to access personal content they may post. Staff should maintain a clear boundary between personal and professional communication and use a privacy setting on personal accounts so that these are not accessible to children.

- have security settings to the maximum
- do not allow any Enfield Learning Trust children or Enfield Learning Trust parents to see their profile
- do not use their profile to bring the school or an individual into disrepute (including children, parents, governors and staff)
- staff must not use their personal mobile or personal device during working hours e.g photography on personal mobile
- disciplinary action may result if these boundaries are not adhered to

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

Further GDPR Guidance & Information can be found in the following polices:

- Data Protection Policy
- Code of Conduct
- Privacy Notices
- Management of Records and Guidance Information

Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding and Child Protection policy.

- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher and the Trust will be informed immediately and action will be taken in line with the Safeguarding and Child Protection policy.

Copyright Issues

It is recognised that all materials on the internet are subject to copyright, unless the copyright is specifically waived. It is the Trust's policy that the copyright of internet materials will be respected.

Where materials are published on the internet as part of the teacher's professional duties, copyright will remain with the Trust. Internet published materials will contain due copyright acknowledgements for any third-party materials included within them.

Useful Resources for Staff:

Cyberbullying
www.cyberbullying.org

Think-U-Know
www.thinkuknow.co.uk

GDPR
https://ico.org.uk/for-organisations/guide-to-data-protection