Queensbridge Online Safety Policy

Creating Future Stars!!

Queensbridge Primary School is a safe, welcoming and nurturing school that offers a sense of belonging. We work with families to ensure that all achieve their potential across our diverse community having relentless high expectations of ourselves and others.
We are innovative, creative and consistent in our approach, constantly reflecting on our practice. We try to make learning creative, stimulating, inclusive and fun with lots of challenge setting ambitious goals for the future.

We try to provide a vast range of opportunities to light the spark of their learning giving them the skills and tools they need to take off and fly!

Queensbridge ensures that children are ready for the world ahead of them as:

- Independent thinkers, enterprising and creative
- Problem solvers, negotiators, reflective and thoughtful
- Excellent communicators
- Happy, confident and curious learners, inspired and well-motivated
- Hard workers
- Responsible members of the community
- Good citizens- children who are respectful, responsible, kind and caring

Happy children make good learners!

Policy Aim

This policy has been written to ensure that the school's ethos, curriculum, and practices promote shared values. It also encourages staff, children and other members of the Queensbridge community to understand others and to value diversity, irrespective of gender, race, belief and sexual orientation.

Policy First written – March 2011 – Reviewed July 2014 – Reviewed February 2015 – reviewed October 2018

Queensbridge Primary School online safety group members

Governing Body Member: Dipti Mouj

SMT member: Sarah Bailey

Online Safety Lead: Afet Nasif (Computing Coordinator)

Child Protection member: Lydia Stober (Assistant Head Teacher)

Data Protection Officer: Sophie Wood – Head of Teaching School

Parent representative: Dana Nayak

Pupil representatives: Digital Leaders

What is online safety?

Online safety is defined as being safe from risks to personal safety and wellbeing when using any device that allows access to the internet.

It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others. This includes personal computers, laptops, mobile phones, tablets and games consoles such as Xbox, PlayStation and Wii.

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour or exploitation.

Safeguarding against these risks is everyone's responsibility, and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the school community, particularly those that are vulnerable.

The term 'safeguard' is defined for the purposes of this document in relation to online safety as the process of limiting risks to children when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection.

Online safety policy statement

The aim of this policy is to ensure children, staff, governors, students and volunteers use the school's internet and Information and Communication Technology (ICT) equipment safely and appropriately, ensuring the best possible outcomes for our children.

The main areas of risk for our school community can be summarised as follows:

Content:

- exposure to illegal, inappropriate or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language);
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content.

Contact:

- being subjected to harmful online interaction with other users;
- grooming;
- child sexual exploitation
- cyber-bullying in all forms;

- extremism and radicalisation
- identity theft and sharing passwords.

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm;
- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (socialising, watching video or gaming);
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- copyright (no thought or consideration for intellectual property and ownership – such as music and film).

Scope

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

The Education and Inspections Act 2006 empowers Head teachers, 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 online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, and is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and the deletion of data.

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 online safety behaviour that take place out of school.

This policy has been created in line with the statutory guidance document **Keeping Children Safe in Education, 2015.**

See appendix for description of roles and responsibilities.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom.
- Policy to be part of school induction pack for new staff.
- School will provide a 'Safe Internet' page for parents on the school website. Information will include internet safety advice, home web filtering tips and links to recommended online safety websites; and guidance on the amount of time children may spend on a computer, smartphone, tablet or games console;
- Acceptable Use agreements discussed with pupils and their families at the start of each year
- Acceptable Use agreements to be issued to whole school community, usually on entry to the setting;
- Children and teachers will be provided with training in the area of online safety.

Handling complaints

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access;
- Staff and pupils are given information about infringements in use and possible sanctions; Sanctions available include:

- interview/counselling by Online Safety Lead / Head teacher;
- informing parents or carers;
- removal of internet or computer access for a period;
- referral to Local Authority, Children's Social Care and/or police.

- Our Online Safety Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher;
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy; Complaints and/or allegations related to child protection are dealt with in accordance with the school and Local Authority child protection procedures:

Review and Monitoring

The online safety policy is referenced from within other school policies: Child Safeguarding and Child Protection policy, Anti-Bullying policy and Personal, Social and Health Education policy.

- The school has an online safety Lead who will be responsible for document ownership, review and updates;
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school;
- The online safety policy has been written by the school online safety Coordinator and is current and appropriate for its intended audience and purpose;
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school Online Safety policy will be discussed in detail with all members of teaching staff;

Named online safety lead – roles and responsibilities

Queensbridge Primary School recognises that **Online safety is a whole school responsibility** and has accordingly set up an online safety group with representation from within the school. Their role is crucial to developing and maintaining an online safety culture. The current members of the online safety group are outlined on the first page of this policy.

The responsibilities of this group are to:

a. Develop an online safety culture at Queensbridge Primary School;
b. Be the named points of contact on all online safety issues;
c. Ensure online safety is included as part of the induction procedures and an Acceptable Use Policy is signed and dated by staff and volunteers;
d. Monitor online safety, such as:
    1. ensuring the infrastructure of technology provides a safe and secure environment for children, for example by ensuring web address filters and other software security are in place;
    2. maintaining an online safety incident log to record concerns and incidents;
e. reporting on online safety issues to the senior management team & governors
f. Ensure that all staff including volunteers and governors members know what to do if they are concerned about an online safety issue;
g. Keep abreast of developing online safety issues via: http://www.saferinternet.org.uk/
h. Ensure that online safety is embedded within continuing professional development (CPD) for staff and volunteers, and co-ordinate training as appropriate;
i. Ensure that online safety is embedded across all activities as appropriate;
j. Ensure that online safety is promoted to parents/carers, children and others in the setting, the home and the community;
k. Review and update online safety policies and procedures on a regular basis and after an incident.

Definitions

What do we mean by 'online'?

When we refer to being online we mean being connected to the internet or communicating through a wide range of devices or technologies, such as computers, laptops, mobile phones, tablet computers, hand-held devices and games consoles.

Setting

Includes any Early Years and childcare provision for children from birth to five, and any out of school provision for children and young people, such as playgroups, pre-schools, childminders, nurseries, Children's Centres and after-school clubs.

Other definitions

The term parent/carer refers to any individual who has a parental responsibility for a child or has care of a child.

Use of ICT equipment

Children should never be allowed to use the internet in the setting without adult supervision

Staff who use the school's ICT and communications systems:

a. Must sign an Acceptable Use Policy;
b. Must use the systems responsibly and keep them safe;
c. Must maintain safe professional boundaries with parents. This includes not giving their personal email address to school users or befriending school users on social network sites such as Facebook;
d. Must treat as confidential any passwords provided to allow access to all ICT equipment;
e. Must ensure integrity of passwords and not share passwords with other members of staff. Network user account passwords should be strong (mixture of letters, number and characters) and be changed periodically, e.g. monthly. If a password is compromised, it must be changed as soon as possible and reported to Data Protection Officer (DPO) in line with current GDPR legislation.
f. Must not install software on the school's equipment, including freeware and shareware without the explicit consent of the DPO.
g. No personal devices (e.g. USB memory sticks) should be used to upload or download material from the school network or website, or any ICT device without the explicit consent of the DPO.
h. If staff require access to digital material offsite, explicit consent must be sought from the DPO and the school will provide appropriate encrypted equipment to do so.
i. Must comply with any ICT security procedures governing the use of systems in the school, including anti-virus measures;
j. Must report known breaches of this policy, including any inappropriate images, messages or other material which may be discovered on the school's ICT systems;
k. Must ensure that the systems are used in compliance with this online safety policy;
l. Staff, volunteers and children will be provided with training in the area of online safety.

Online safety and use of digital devices

At all times, children, staff, Governors, Parents, students and volunteers will treat others with respect and will not undertake any actions that may bring the school into disrepute. The use of personal mobile phones by staff and pupils around school is not allowed for the following reasons:

a. Mobile/smartphones and personal devices can allow wireless and 3G/4G internet access via alternative ISPs, and therefore bypass the school's central security settings and filtering;

b. Mobile/smartphones with integrated cameras could lead to child protection, bullying, and data protection issues with regard to inappropriate capture, use or distribution of images of children or staff.

Equipment

All computer equipment is installed professionally by the school's ICT technicians and meets current health and safety standards. Equipment is maintained to ensure health and safety standards are followed.

Internet access

School's Internet Service Provider (ISP) is London Grid for Learning (LGfL). LGfL is a Regional Broadband Consortium, and provides services to the majority of schools across the 33 boroughs of London via its partnership with Virgin Media Business.

Email access

School uses Hackney Learning Trust Outlook email to detect and block viruses, spam, phishing, Trojan, and other malicious message types, and inappropriate language.
All staff agree to:

a. Only use standard school-issued email addresses for work related communication and professional use;
b. Staff, volunteers, Governors and all those connected professionally with school will not send material that is illegal, obscene, upsetting or defamatory, or that is intended to annoy or intimidate another person. Should such content be received, it must not be forwarded to anyone, and must be reported to the online safety co-ordinator and the DPO, who will take appropriate action;
c. Are aware that spam, phishing, Trojan and virus attachments are a danger to the school's systems.

Digital images, School website, App, Social Media

International evidence states the greatest impact on a child's learning is the extent of parental engagement in their children's education. Here at Queensbridge Primary School we use our website, social media and YouTube to explain our curriculum and classroom work to parents via web pages, blogs, direct tweets and videos. We believe that the public nature of the work provides extra motivation for learners and in addition:

- Provides vital information to parents, empowering them to start a conversation with their child about their learning.
- Allows children to direct parents to their work showcased on the school website. Provides teachers with a forum to publish work that children are proud of online thereby offering additional incentives
- Gives school the opportunity to demonstrate and model safe and respectful ways to use online media

We believe that with social media becoming increasingly part of everyday life it is important to stress that all members of our community should take responsibility for their online presence, respecting the opinions and privacy of others and modelling good behaviour to our children.

To comply with GDPR legislation, your permission will be sought before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images: If the pupil is named, we avoid using their image. If their image is used, we avoid naming the pupil. Where showcasing examples

of pupils work we only use their first names, rather than their full names. If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Only images of pupils in suitable dress are used.

a. Children's learning will be published on the school website, and other school online spaces
b. The website will be edited only by members of staff approved by the Head Teacher. All information placed on the website must adhere to the ethos and values of the school's online safety Policy
c. Personal pupil information including home address and contact details will be omitted from school web pages;
d. The school website will not publish the surnames of any pupils;
e. The school will ensure that the image files are appropriately named – and do not use pupils' names in image files if published on the web;
f. School will ensure the web hosting company has a published security protocol

Data security and GDPR

a. Personal data is stored securely. Access to personal data is strictly controlled by the Designated Safeguarding Lead and the DPO;
b. Data is secured against loss failure, theft and damage through systems and policies as set out in the GDPR policy
c. If personal or sensitive data, needs to be transmitted, it is done so securely as outlined in the GDPR policy.
d. An incident management log is maintained by the DPO.
e. Data security incidents must be reported through the appropriate internal management channels as set out in the school's GDPR Policy;
f. Serious incidents of data breaches should be reported to the DPO who will in turn inform the Information Commissioner's Office;
g. All electronic equipment that is to be reused or disposed of will have all of its data and software erased/destroyed, in accordance with the current policy and as set out in the GDPR policy.

Mobile phones

a. Staff should not have personal mobile phones on them when they are working with children in school. These conditions also apply to students and volunteers;
b. Staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the setting in a professional capacity;
c. Parents, carers and visitors are requested not to use their mobile phones while on the school premises. School staff will remind parents, carers and all visitors of the policy by reminding them to switch off their phones when they enter the setting or asking them to leave the rooms to make or receive calls in the reception area when necessary.

Digital cameras /iPads/other devices

- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils or other members of staff, and will only use work-provided equipment for this purpose;
- Parents/Carers receive a Digital Images, Website and Social Media Agreement as part of their welcome pack to the school. Queensbridge School must obtain explicit consent from parents in order to photograph their children.
- Personal cameras are not allowed in school without prior agreement of SMT, and should not be used on off-site activities, home visits and outings;
- The school offers staff school iPads to all teachers to take photographs of children for display, observations or profile books;
- No one is permitted to photograph or record images in the toilet and changing areas;

- Photographers will be required to have clear formal identification which must be worn at all times, for example at an open day or event;
- Queensbridge Primary School requests explicit permission from parents in order to use images of their children on the school website, app or other social media channels and social networking sites
- Internet access at school will always be overseen by a member of staff;
- Children's access to websites are limited to those agreed by the school only;
- School staff and volunteers will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials on school equipment;
- School staff will report accidental accessing of inappropriate materials in accordance with school procedures;
- Staff, volunteers and children will use the Internet for educational purposes only;
- Downloading materials or images not relevant to teaching and learning is in direct breach of school policy;
- School staff will be aware that all internet activity, including distributing or receiving information, school-related or personal, will be monitored for unusual activity, security and/or network management reasons;
- Staff are instructed not to share their own personal online spaces with their pupils or the pupils' families and to take the appropriate steps to protect their privacy.
- Staff must not search for, visit or monitor social networking presences of pupils or families.
- If a staff member does happen to find such a social network site or presence, they must not enter them. This is uninvited intrusion into a family's life, and you and your employer are liable to investigation if you act outside these guidelines. If you have safeguarding/child protection concerns about a child's/young person's behaviour on-line, or if you think a social media platform could provide critical information, for example, if a child is missing or is at risk of harm, the police and children's social care must be contacted. If warranted, the only agency that can access these sites is the police.

a. School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community or the setting's activities in any negative context, and/or actions that may bring an individual, profession or setting's reputation into disrepute
- Personal opinions should not be attributed to the school or Local Authority;

Responding to Incidents

Policy statement

- When an online safety incident occurs, members of staff should report this to the online safety officer (for more detailed information please refer to 'What do if' Appendix 1).
- All incidents, whether involving pupils or staff, must be recorded by the online safety officer using the online safety incident report form a copy of which can be obtained from the online safety office
- Where the incident or complaint relates to a member of staff, the matter must always be referred to the Head teacher for action. Incidents involving the Head teacher should be reported to the chair of governors.
- The school's online safety officer should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy.
- Online incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection lead of the online safety group,

who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.

- Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither Queensbridge Primary School nor the London Borough of Hackney can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional access of inappropriate websites

- If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) minimise the screen.
- Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.
- The incident should be reported to the online safety officer and details of the website address and URL provided together with a screen-shot where possible
- The online safety officers should liaise with the IT technician to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.
- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (e.g.: sex education) that they notify the IT technician so that filtering can be put back to minimise the risk of inappropriate sites being accessed by pupils or staff.

Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see Sanctions section).
- The incident should be reported to the online safety officers and details of the website address and URL recorded.
- The online officers should liaise with the IT technician to ensure that access to the site is blocked.
- The pupil's parents should be notified of the incident and what action will be taken.

Inappropriate use of ICT by staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Head teacher and the online safety officers immediately.
- The online safety officers should notify the IT technician so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.
- The online safety officer should arrange with the IT technician to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established, the Head teacher should take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.
- If the materials viewed are illegal in nature the head teacher should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.

Cyber bullying

Definition and description

Traditionally, bullying took place face to face in the physical world; on-line, bullying can take on a new dimension with technologies such as text, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Types of cyberbullying
There are many ways of bullying someone online and for some it can take shape in more ways than one. Some of the types of cyber bullying are:

- **Harassment** - This is the act of sending offensive, rude, and insulting messages and being abusive. Nasty or humiliating comments on posts, photos and in chat rooms. Being explicitly offensive on gaming sites.
- **Denigration –** This is when someone may send information about another person that is fake, damaging and untrue. Sharing photos of someone for the purpose to ridicule, spreading fake rumours and gossip. This can be on any site online or on apps.
- **Flaming** – This is when someone is purposely using really extreme and offensive language and getting into online arguments and fights. They do this to cause reactions and enjoy the fact it causes someone to get distressed.
- **Impersonation** – This is when someone will hack into someone's email or social networking account and use the person's online identity to send or post vicious or embarrassing material to/about others.
- **Outing and Trickery** – This is when someone may share personal information about another or trick someone into revealing secrets and forward it to others. They may also do this with private images and videos too.
- **Cyber Stalking** – This is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for his or her safety. The actions may be illegal too depending on what they are doing.
- **Exclusion** – This is when others intentionally leave someone out of a group such as group messages, online apps, gaming sites and other online engagement. This is also a form of social bullying and a very common.

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- Queensbridge Primary School will not tolerate any act of cyber-bullying. Any incidents will be dealt with in-line with the school's behaviour and anti-bullying policies (See the Behaviour Policy and Anti-Bullying Policy)
- Any incidents of cyber bullying should be reported to the online safety officer who will notify record the incident on the incident report form and take appropriate steps to deal with the incident in line with the school's Anti-Bullying Policy. Incidents will be monitored and the information used to inform the on-going review and development of anti-bullying policies.
- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, they will be reported to the police as in these cases, the bullying may be a criminal offence.
- As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.
- Pupils should be taught:

    - to only give out personal details to people they trust
    - to only allow close friends whom they trust to have access to their social networking sites
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.
    - to preserve evidence of bullying, for example texts, instant messaging or comments on websites

Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The pupil should also consider changing their phone number.
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The pupil should also consider changing email address.
- Where bullying takes place in chat rooms, the pupil should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
- Where bullying involves instant messages, social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
- Parents should be notified of any incidents where the school have been made aware that their children are affected and advised on what steps to take to block further abuse
- on devices at home.

Cyber bullying of teachers

- Head teachers should be aware that teachers may become victims of cyber bullying by pupils. Because of the duty of care owed to staff, Head teachers should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils.
- Incidents of cyber bullying involving teachers should be recorded and monitored by the online safety officers in the same manner as incidents involving pupils.

- Teachers should follow the guidance on safe ICT use in this policy. Staff should not use their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.
- Private contact details for teachers should not be posted on the school website or in any other school publication.
- Teachers should follow the advice above on cyber bullying of pupils and not reply to messages but report the incident to the head teacher immediately.

Risk from inappropriate contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

- All concerns around inappropriate contacts should be reported to the online safety officers and the designated child protection teacher.
- The designated child protection teacher should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
- The designated child protection teacher can seek advice on possible courses of action from CEOP.
- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.
- The designated child protection teacher and the online safety officers should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.
- Where inappropriate contacts have taken place using school ICT equipment or networks, the online safety officers should make a note of all actions taken and contact the school's IT technician to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimal

Teaching and Learning

Guidance on teaching online safety

Responsibility

One of the key features of the Queensbridge online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the online safety officers, but all teaching staff are expected to play a role in delivering online safety messages as part of the Computing Curriculum Programme of Study. Computing Curriculum Coordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

Content

Pupils should be taught:

- About the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that the school has a “no blame” policy so that pupils are encouraged to report any online safety incidents
- that the school has a “no tolerance” policy regarding cyber bullying
- the basic principles of “netiquette”
- behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- the school’s ICT resources should only be used for educational purposes
- LGFL has been designed so that use is monitored and that access to some sites are blocked
- the school’s policy on using their own mobile phones whilst in school.

Delivering online safety messages

- Teachers are primarily responsible for delivering an on-going online safety education in the classroom as part of the Computing Curriculum Programme of Study.
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.
- The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles in order to keep safe.
- Teachers may wish to use PSHE lessons as a forum for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author’s view is objective and what authority they carry
- carrying out comparisons with alternative sources of information
- considering whether the information is current and whether the facts stated are correct.

In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

Conclusion

The school recognises that the use of the technology, including access to the internet and ICT devices, can substantially and positively impact the quality of teaching and learning of our children and staff. This policy aims to ensure that such use is done safely and appropriately

Online Safety Guidance: What to do if…

Online Safety Group:

Governing Body Member: Dipti Mouj

SMT member: Sarah Bailey

Online Safety Lead: Afet Nasif (Computing Coordinator)

Child Protection member: Lydia Stober (Assistant Head Teacher)

Data Protection Officer: Sophie Wood – Head of Teaching School

Parent representative: Dana Nayak

Pupil representatives: Digital Leaders

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

An inappropriate website is accessed unintentionally in school by a teacher or child.
1. Play the situation down; don't make it into a drama.
2. Report to a member of the online safety group and decide whether to inform parents of any children who viewed the site.
3. Incident to be logged using the school's online incident report proforma
4. Inform the school technician and ensure the site is filtered.
5. Inform LGFL about the website.

An inappropriate website is accessed intentionally by a child.
1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions. Record incident in-line with behaviour policy and online incident report form as appropriate
2. Report to online safety group
3. Notify the parents of the child.
4. Inform the school technician and ensure the site is filtered if need be.
5. Inform LGFL about the website.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you. Do not view the misuse alone.
2. Report the misuse immediately to the head teacher and online safety officer. Ensure that there is no further access to the PC, laptop or equipment and evidence is saved.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the device to a secure place.
    - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).
    - Inform governors of the incident.
    - In an extreme case where the material is of an illegal nature:
    - Contact the local police or High Tech Crime Unit and follow their advice.
      If requested to, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online safety, anti-bullying, PHSE and AUP. Apply appropriate sanctions.
3. Report to online safety group.
4. Secure and preserve any evidence. Ask for IT technician's help if necessary.
5. contact the website provider to request that the comments are removed.
6. Notify parents of the children involved.
7. Consider delivering a parent workshop for the school community.
8. Inform the police if necessary, and send all the evidence to Child Exploitation & Online Protection Centre (CEOP at www.ceop.gov.uk/contact_us.html)
9. Inform the LA online safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Report to online group
2. Secure and preserve any evidence.
3. Send all the evidence to Child Exploitation & Online Protection Centre (CEOP at www.ceop.gov.uk/contact_us.html)
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform and request the comments be removed if the site is administered externally.
6. Inform LA online safety officer.
7. The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the CP, online safety group and Head teacher in school, and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/ (Child Exploitation & Online Protection Centre - internet safety).
4. Involve the police and social services if the child is in immediate risk.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be recorded and reported immediately to the online group and Head Teacher.