Blue Gate Fields Infant School
Learn | Grow | Achieve

Blue Gate Fields Infant School

E-Safety Policy

Agreed by staff and Governors

Date: October 2019
Review Date: October 2020

This policy is the responsibility of the Head teacher with the ICT manager

Managing the Internet safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils are taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to children and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- secure data exchange between local and government bodies.

The risks

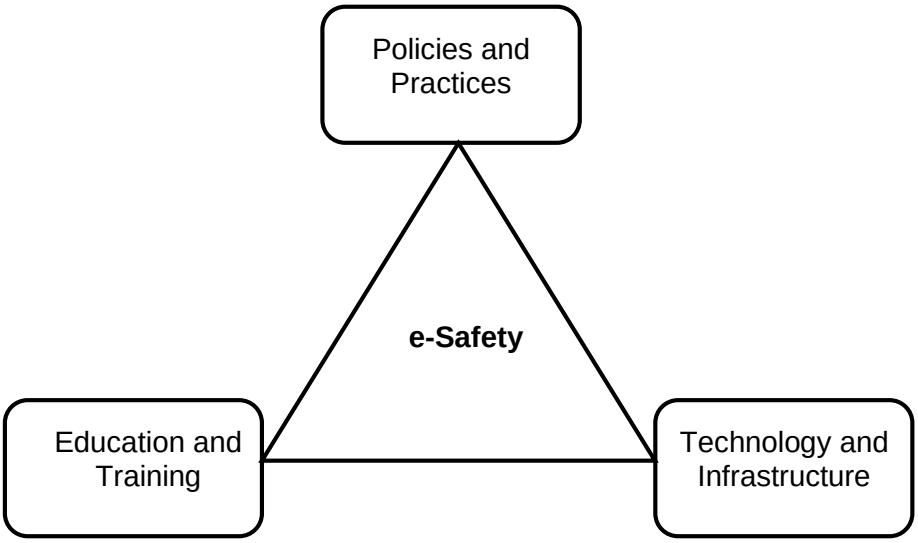
- The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.
- Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.
- Our E-safety policy ensures that children are provided with an Internet environment which is as safe as possible. We teach children to be aware of and respond responsibly to any risk. There is a 'No Blame', supportive culture and

children are supervised when using the internet. Children are taught to report any abuse to an adult.

- The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984). Staff are aware of the need to use all computer and electronic equipment responsibility, and sign the 'Acceptable Use' policy.

There are three aspects to E-safety.

1. Technology
2. Policy and Practices
3. Education and Training



1.Technology and infrastructure:

Blue Gate Fields Infant School:

- Uses the London Grid for Learning (LGfL) who procure the broadband supply from Virgin Media Business.
- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Works in partnership with the LGFL to ensure any concerns about the system are conversed to the correct person/department at Atomwide or LGFL.

- Ensures network health through appropriate anti-virus sand anti-spyware software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures the Systems Administrator / Network Manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / Network Manger checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Either uses a child friendly search engine such us kiddle, swigle or Google under adult supervision.

Sanctions and infringements

All staff read and sign the Acceptable Use Policy. Failure to comply with the policy will be managed under the school disciplinary procedures. In the future parents will be asked to sign an E Safety agreement as part of the Home School Agreement.

2. Policy and procedures

This school:

- Supervises children's use at all times.
- Does not allow aimless surfing of the Internet.
- Uses the pan-London LGfL / Virgin Media Business filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Requires staff to preview all sites before use
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Headteacher.
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Does not currently use any webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;

- Teaches children to use the internet safely. Pupils only use email through an approved school email address supervised by an adult.
- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- Requires staff to make sure that E-mails sent to external organisations should be written in the same way as a letter written on school headed paper.
- Does not permit forwarding of chain messages.
- Informs staff that they should not use personal email accounts during school hours or for professional purposes. (this reinforces what is already in the AUP)
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Ensures parents understand that children use the internet under supervision in school.
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material suspected to be illegal to the appropriate authorities e.g. police or LA.
- When staff and pupils leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.

3. <u>Education and training:</u>

This school:

- Fosters a 'No Blame' environment that encourages children to tell a responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; they should be taught to say where they have downloaded information from.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate, e.g. not opening adverts etc.
- Runs a rolling programme of advice, guidance and training for parents, including:
    a. Information leaflets; in school newsletters; on the school web site;
    b. demonstrations, practical sessions held at school;
    c. distribution of 'think u know' for parents materials
    d. suggestions for safe Internet use at home;
    e. provision of information about national support sites for parents.

Managing Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any activity on the network including internet and email activity.

The Headteacher and governors have responsibility to ensure that:

- All staff understand their responsibilities relating to managing equipment.
- The network is set-up so that users cannot download executable files / programmes;
- Inappropriate sites are blocked. We follow LA advice on using filters and use the LGFL filters as standard.
- Access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.
- Equipment is maintained in accordance with Health and Safety guidelines.
- We review the school ICT systems regularly with regard to security.
- We ensure that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
- We do not allow any outside Agencies to access our network remotely.

Procedure statements

All staff:

To ensure the network is used safely in this school all staff will:

- Read and sign that they have understood the school's e-safety Policy. Staff understand that the use of the internet is monitored in school.
- Take responsibility for turning off computers and smart screens & projectors at the end of the day.
- Ensure that members of staff do not log on as another user – if two people log on at the same time this may corrupt personal files and profiles. Staff must not share their passwords with others.
- Understand how to use the network which has a shared work area for pupils and one for staff.
- Always log off when they have finished working or are leaving the computer unattended.
- Log off any computer which has been inadvertently left on and log in as themselves if they wish to use the computer.
- Understand that they are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date.
- Scan all mobile equipment with anti-virus / spyware before it is connected to the network;
- Understand that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Follow the guidelines set out in the General Data Protection Regulations 2018 when accessing, amending and saving any data or information, relating to the school or pupils.

Procedure statements:

Teachers and support staff (nursery nurses and teaching assistants)

All teachers and support staff will:

- Ensure that pupils are taught to log in to their individual class area on the server.
- Log on as 'teacher' and ensure that pupils log on as 'pupil' on individual computers.

- Ensure that pupils are never allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage/delete files or the network;

- Ensure that pupils do not have unattended access to the computer which is logged in as teacher.

- Images that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Staff will not use mobile phones during lessons or formal school time.

Cyberbullying/electronic bullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

Procedure statements:

Administrative staff

All administrative staff will:

- Ensure that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA;
- Be aware of security guidelines when accessing secure data and set their computers to 'time out' after 15 minutes of not being used, re-entering their user name and password to re-enter the site.
- Use the DfES secure s2s website for all CTF files sent to other schools;
- Ensure they log off of their computer when they are not using it, or not near to it.
- Adhere to GDPR guidelines to maintain confidentiality.

Procedure statements:

Children

All children will:

- Log on to their own class area using their class username and password.
- Not share their class passwords with others.
- Take part in e-safety sessions.

E-safety – Complaints

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

Staff acceptable use

This policy is comprehensive and covers the use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my username & password(s) combination to anyone.
- I will not allow unauthorised individuals to access email / Internet / network /printers, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (currently: London Grid for Learning Mail (LGFL) http://mail.lgflmail.org.)

- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the head teacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that the data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I agree to abide by all the points above.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …… Date……..

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature Head Teacher

I approve this user to be set-up.

Signature ..... Date.....

Full Name ..... (printed)

This policy on E Safety was approved by governors in November 2019 and signed by the chair of governors.

…….. ……. Chair of governors.

…… Date

It will be reviewed in November 2020 or sooner in the case of new information, changes or legislation.