Bowlee Park Community School

Online-Safety Guidance
and
Acceptable Use Policy

Introduction

The e-Safety Policy is important in school for a number of reasons, including:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set boundaries of use (goalposts) of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. blogging, Twitter).

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

- **Users** - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.
- **Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
- **School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Safeguarding is a serious matter; at Bowlee Park Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Bowlee Park Community School staff area; upon review all members of staff will read both the e-safety policy and the Staff Acceptable Use Policy.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least every two years and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- A dedicated E-Safety governor (Safeguarding Link governor) will be available in the instance where a serious E-Safety breach has occurred. The named E-Safety Governor is Collette Radcliffe. In such an event the E-Safety team will meet to investigate, resolve or escalate the issue.

Headteacher
Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, DSL/ICT Manager, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The ICT Technical team and DSL has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- Bowlee Park has two trained CEOP Ambassadors in school (Carole Smith and Sarah Anderson).

DSL/DDSL/ICT Manager
Will:

- Keep up to date with the latest risks to children whilst using technology; familiarize themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff
Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age.

All Staff
Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is recorded on CPOMS. If you are unsure the matter is to be raised with the DSL or the Headteacher to make a decision.

All Students

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

The Teaching online Safety in School Document 2022 states that "It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app"

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through school newsletters, the school website the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded.

Technology

Bowlee Park Community School uses a range of devices including PC's, laptops, IPads and Chromebooks. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Fortigate software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Manager and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Fortigate software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998 and GDPR 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the

local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device without a username and password. Staff are expected to keep their passwords private. The ICT Manager and IT Support will be responsible for ensuring that passwords are changed if needed.

Passwords must adhere to the following security protocol:

- At least 14 characters
- At least 1 capital letter
- At least 1 special character
- At least 1 number

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff and students in accordance with school policy

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip. Non return of the slip assumes permission has not been given.

Social Networking – there are many social networking services available; Bowlee Park Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Bowlee Park Primary School. Should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter- used by authorized staff in school
- Facebook – used by authorized staff in school

A broadcast service is a one-way communication method in order to share school information with the wider school community.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.

- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the DSL/DDSL via CPOMS, or in his/her absence the Headteacher. The DSL will assist you in taking the appropriate action to deal with the incident.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Bowlee Park Primary School will have a programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Every half term, pupils are taught about e-safety, before the beginning of a new unit of Computing. We use various resources and websites, particularly the SMART information.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The DSL is responsible for recommending a programme of training and awareness for the school year. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Reviewed: September 2024
Next Review: September 2026