Ballyowen Meadows Special School

DIGITAL MEDIA ACCEPTABLE USE & E-SAFETY POLICY

Contents

INTRODUCTION

Ballyowen Meadows Special School believes in the benefits of the curriculum-based use of digital media. The purpose of this Digital Media Acceptable Usage Policy is to ensure that pupils will benefit from learning opportunities offered by the school's digital resources, and will be protected from harmful and illegal use of the Internet.

This policy covers online safety and provides local rules around digital devices, which apply equally to mobile/portable devices (i.e. Laptops, mobile phones, tablets, hand held devices). All portable devices used within the school are covered by this policy irrespective of ownership.

ALIGNMENT WITH CHARACTERISTIC SPIRIT OF BMSS

This policy has been developed in consultation with key stakeholders, i.e. Board of Management, Parents and School Staff, for the purpose of ensuring that it is understood by everyone that there is a shared responsibility in ensuring that children are safe when using digital media. This partnership approach to E-Safety is particularly important for pupils attending BMSS as they have an increased level of vulnerability when using digital media.

In addition, the degree to which access to digital media technology is permitted for each child is personalised with consideration given to the child's special needs. In addition to a curriculum tool, digital technology may form part of a child's behaviour plan as a reinforcer. However, consideration of the addictive nature of technology for some pupils will also be considered when the level of access is decided.

AIMS

The purpose of this policy is to safeguard and protect all our young people and staff when using digital media. This document specifies the expectations for all key stakeholders and is supplemented by additional documentation available on the school's cloud storage system (Staff) and school website (Parents).

RESPONSIBILITIES OF KEY STAKEHOLDERS

(1) PARENTS

The school expects all Parent(s)/Guardian(s) to support the school in promoting E-Safety and in enabling the school to safeguard all its stakeholders. The school provides advice and guidance on its website. Parents and carers are welcome to contact the school if they need any help or advice in supporting the safe use of IT and online safety.

Parents will also be required to give permission on the BMSS Parent Permission Form before their child can access Digital Media Technology in school.

(2) BOARD OF MANAGEMENT

The main risks to the school have been identified to the Board of Management during the BMSS Digital Media Usage Risk Assessment and encompasses the following:

- inappropriate content
- hate sites
- cyber-bullying
- grooming
- sexual content
- extremism and radicalisation
- identity theft and privacy
- breach of copyright
- reputational damage to the school and its stakeholders

There are three core ways to mitigate risks to consider:

- Acceptable use of digital media technology
- Policies and practices
- Education and training

In addition, BMSS manages these risks through the following means:

- internet content filtering;
- secure filtered and anti-spammed email services;
- protecting personal data;
- managed internet content;
- no access to social media;
- educating our pupils;
- staff and parents training;
- use of permissions for images and videos;
- additional access control to networks;
- effective and timely reporting of issues;
- effective supervision of use of IT within the curriculum;
- weekly web access reporting.

All online access is filtered and every effort is made to prevent inappropriate materials from being accessible. Owing to the size and complexity of the internet, the school and its internet services providers are unable to guarantee complete filtering. The school maintains the right to monitor all internet access and online activity and may take appropriate action. Incidents are managed locally by members of the In-School Management Team (ISMT) and are reportable as safeguarding concerns. Key stakeholders are provided with training, advice and guidance as to the safe and effective use of digital media technology on a continual basis.

(3) SCHOOL STAFF

As a professional organisation with responsibility for children's safeguarding it is important that school staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.

This policy informs members of BMSS staff to ensure that they are fully aware of their professional responsibilities when using Information Communication Technology and the school systems.

Staff should be alert to the following acceptable use guidelines and use the relevant school procedures when required:

ACCESSIBILITY:

- Staff must read, know and adhere to the contents of this Digital Media Acceptable Use Policy. Staff are also asked to sign the BMSS Staff Acceptable Use Policy Adherence Form indicating their agreement to abide by this policy.

- All staff members are individually responsible for ensuring they have read and understood this policy and how it is applied in the workplace.

- Each staff member must return the BMSS Acceptable Use of Digital Media Technology stating that they have read, understood and agree to adhere to all guidelines and assume responsibility for their own actions.

- Staff must keep their user password secure and confidential.

- Staff must provide their passwords to the School Principal for purposes of oversight. These passwords will be stored securely.

- Staff must not access inappropriate materials at school when using school owned or personal devices or when using school owned devices when working outside school. Doing so will lead to disciplinary action being taken.

- Staff should ensure that devices are being legally used according to the software's licence.

- Staff should only install software onto a school computer or network with prior approval by the School Principal.

USAGE:

- BMSS computers and networks must be used in a responsible, efficient, ethical and legal manner and must be in support of the educational objectives of our school. The School Management reserves the right to monitor this usage.

- Incidental personal use of school computers is permitted as long as such use does not interfere with the employees' role, duties and performance with system operations or other system

users. 'Incidental personal use' is defined as use by an individual employee for occasional personal communications.

- Staff must not transmit, request or receive materials inconsistent with the BMSS Ethos, Vision and Value Statement.

SAFEGUARDING:

- Each staff member has a duty to report any online safety concerns, including safeguarding concerns, to the School Principal/ Designated Liaison Person (DLP) or Deputy Principal.

- All staff are accountable for ensuring that pupils and other key stakeholders are safeguarded at all times when online.

- Pupils should be closely supervised at all times when accessing and using digital media technology.

- Staff should model and provide instruction in the ethical and appropriate use of technology in a school setting.

- All Staff are responsible for ensuring that a curricular focus is maintained.

- All staff should ensure that the pupils with whom they work have permission given by their parent allowing them to access technology when in school.

E-SAFETY – TEACHING AND LEARNING STRATEGIES:

BMSS will employ a number of strategies to maximise learning opportunities and reduce risks associated with the use of Digital Media when in school. This is not an exhaustive list and all members of staff are reminded that ICT use should always be consistent with the school ethos, other appropriate policies, DES requirements and legislation.

INTERNET

- Internet will be used for educational purposes only
- Internet sessions will always be supervised by a teacher
- Pupils will seek permission before entering any Internet site, unless previously approved by a teacher
- Filtering software will be used to minimise the risk of exposure to inappropriate material
- The school will regularly monitor pupils' internet usage
- Pupils will receive training in the area of internet safety
- Pupils will be taught to evaluate the content of internet sites
- Teachers will be made aware of internet safety issues
- Uploading and downloading of non-approved material is banned
- Virus protection software will be used and updated on a regular basis
- The use of personal floppy disks, external storage devices or CD-ROMS are not permitted on school devices.
- Pupils will observe good "netiquette" (etiquette on the internet) at all times and will not undertake any action that may bring a school into disrepute
- 'YouTube' (and similar sites) can be accessed only under the supervision and direction of the teacher.

EMAIL

If pupils are allowed to use email, the following rules will apply:

- Email will be used for educational purposes only
- Students will only use approved class email accounts under supervision by or permission from a teacher
- Pupils will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person
- Pupils will not send text messages to or from school email
- Pupils will not reveal their own or other people's personal details e.g. addresses, telephone numbers, or pictures via school email
- Pupils will never arrange to meet someone via school email
- Sending or receiving email attachments is subject to teacher permission.

INTERNET CHAT

Students are not permitted to use internet chat rooms.

GAMES CONSOLES

Most games consoles are able to access online content. To help ensure adequate levels of online safety, consoles used in the school will not have online access.

SCHOOL WEBSITE

- Designated School Staff will manage the publication of material on the school website.
- Personal pupil information, home addresses and contact details will not be published on the school website
- Class lists will not be published
- Pupils' full names will not be published beside their photograph
- Digital photographs, video clips and audio clips will focus on groups and group activities rather than on individual pupils (apart from circumstances where permission is given by a parent)
- Pupils will be given an opportunity to publish projects, artwork or school work on the school website
- Teachers will select work to be published and decide on the appropriateness of such
- Permission to publish a student's work will be sought from pupils/ parents/ guardians. This permission may be withdrawn at any time.
- Pupils will continue to own the copyright on any work published.

DISTANCE LEARNING

- In circumstances where teaching cannot be conducted on the school premises, teachers may use *Zoom for Education* set up by the school or other platforms approved by the Principal as platforms to assist with remote teaching where necessary.
- The school has signed up to the terms of service of the Online Platforms in use by the school.
- The School has enabled the most up to date security and privacy features which these Online Platforms provide.
- If teachers are using Zoom, parents/guardians must consent to their child having a school email address as above to allow their child access to the lessons. Where the child does not have a school email address, parents can consent by submitting their own email address for their child to access lessons on Zoom.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms.

Zoom Use and Safety:

- Every user must be easily identifiable to the host and others in the meeting by the email address they are using.
- Please ensure that your user name is your child's name or initials. This is for security reasons as we can only admit identifiable pupils to the lesson.
- It is also extremely important that all accessing zoom meetings show a visual presence from a safety perspective. Anyone not prepared to adhere to these guidelines should be advised that they will be left in the zoom 'waiting room' by the host and will not gain access.
- You can leave the lesson at any time if you need to.
- Please mute your microphone where appropriate e.g. if another child, adult or staff member is talking. You can unmute your microphone when it is your turn.
- Please use a quiet room with limited background noise.
- Recording of zoom meetings and lessons or images thereof are not allowed.
- A unique Zoom ID and password for each meeting will be sent to parents and should not be shared for added security. These details will be emailed to parents/staff in advance of each meeting.

UNACCEPTABLE USE:

Unacceptable use of online platforms and the internet will be dealt with under the Code of Behaviour policy.

RATIFICATION

This policy was ratified by the Board of Management on 26 May 2020.

EVALUATION

This policy will be evaluated through the process of the BMSS Acceptable Use Risk Assessment Audit.

REVIEW

The policy will be reviewed as required.