# Margaret McMillan Nursery School and Children's Centre

Hornsey Rise
Islington
N19 3SF
020 7281 2745
www.margaretmcmillan.islington.sch.uk

# Online safety Policy

## Contents

## 1. Introduction and Overview

### 1.1 Rationale

**The purpose of this policy is to:**

- set out the key principles expected of all members of the school community at Margaret McMillan Nursery School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Margaret McMillan Nursery School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

**Content**

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

**Contact**

- grooming
- cyber-bullying in all forms
- identity theft (e.g. 'frape' (hacking Facebook profiles)) and sharing passwords

**Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

### 1.3 Scope

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

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 e-safety behaviour that take place out of school.

## 1.4 Roles and responsibilities

| Role | Key Responsibilities |
|---|---|
| Headteacher | • To take overall responsibility for e-safety provision<br>• To take overall responsibility for data and data security (Senior Information Risk Owner)<br>• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements<br>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant<br>• To be aware of procedures to be followed in the event of a serious e-safety incident.<br>• To receive regular monitoring reports from the E-Safety Co-ordinator / Officer<br>• To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures( e.g. network manager) |
| Online safety Lead (Headteacher) | • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents<br>• promotes an awareness and commitment to e-safeguarding throughout the school community<br>• ensures that e-safety education is embedded across the curriculum<br>• liaises with school ICT technical staff<br>• To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs<br>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident<br>• To ensure that an e-safety incident log is kept up to date<br>• facilitates training and advice for all staff<br>• liaises with the Local Authority and relevant agencies<br>• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:<br>∗ sharing of personal data<br>∗ access to illegal / inappropriate materials<br>∗ inappropriate on-line contact with adults / strangers<br>∗ potential or actual incidents of grooming<br>∗ cyber-bullying and use of social media |
| Governors / Governor with responsibility for Child Protection | • To ensure that the school follows all current e-safety advice to keep the children and staff safe<br>• To approve the Online safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. The Online Safety Governor is also the Safeguarding Link Governor.<br>• To support the school in encouraging parents and the wider community to become engaged in online safety activities<br>• The role of the Online Safety Governor will include:<br>∗ regular review with the Online Safety Lead (including online safety incident logs, filtering / change control logs ) |
| Computing Curriculum Leader | • To oversee the delivery of the e-safety element of the Computing curriculum<br>• To liaise with the online-safety coordinator regularly |
| Network Manager | • To report any e-safety related issues that arise to the online safety coordinator.<br>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed<br>• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date<br>• To ensure the security of the school ICT system<br>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices<br>• the school's policy on web filtering is applied and updated on a regular basis<br>• Respond to issues relating to the filtering applied by the school<br>• keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant |

| Role | Key Responsibilities |
|---|---|
| | • that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation action / and sanction where necessary.<br>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.<br>• To keep up-to-date documentation of the school's e-security and technical procedures |
| Data Manager (headteacher) | • To ensure that all data held on pupils on the school office machines have appropriate access controls in place |
| Teachers | • To embed e-safety issues in all aspects of the curriculum and other school activities<br>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant) |
| All staff | • To read, understand and help promote the school's online safety policies and guidance<br>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy<br>• To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices<br>• To report any suspected misuse or problem to the e-safety coordinator<br>• To maintain an awareness of current e-safety issues and guidance e.g. through CPD<br>• To model safe, responsible and professional behaviours in their own use of technology<br>• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. |
| Pupils | • to understand the importance of reporting abuse, misuse or access to inappropriate materials<br>• to know what action to take if they or someone they know feels worried or vulnerable when using online technology.<br>• To understand the importance of adopting good online safety practice when using digital technologies out of school<br>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home |
| Parents/carers | • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images<br>• to consult with the school if they have any concerns about their children's use of technology. |
| External groups | • Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school |

### 1.5 Communication:

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use discussed with pupils as appropriate.
- To provide Acceptable use agreements in line with school policy and procedures
- Acceptable use agreements to be held in staff personnel files

### 1.6 Handling complaints:

- The school will take all reasonable precautions to ensure e-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 informed of expected conduct in their use of technology. Sanctions may include:
    - interview/advice from E-Safety Coordinator / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system
    - referral to LA / Police.
- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher
- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

### 1.7 Review and Monitoring

The online safety policy is referenced from within other school policies: Child Protection policy and in the School Development Plan, Positive Behaviour policy.

- The school has an online safety coordinator who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed bi-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: Headteacher, school online safety Coordinator and the network manager, it 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. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

## 2. Education and Curriculum

### 2.1 Pupil online safety curriculum

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on national guidance. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line.

### 2.2 Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to protect data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program; through annual updates and regular staff meetings etc
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safeguarding policy and the school's Acceptable Use Policies.

### 2.3 Parent awareness

This school

- Can offer advice and guidance to parents, including:
    - provision of information about national support sites for parents.
    - advice for child internet use:

## 3. Expected Conduct and Incident Management

### 3.1 Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Parents/Carers

- need to be aware of acceptable use of technology within the school setting, particularly in relation to personal technology.

### 3.2 Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local and central government authorities) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

## 4. Managing the ICT infrastructure

### 4.1 Internet access, security (virus protection) and filtering

This school:

- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Applies a user-level filtering where relevant, thereby closing down or opening up options appropriate to the needs of the school.
- Ensures network health through use of anti-virus software
- Uses secured email to receive personal data over the Internet and encrypts personal data when sent over the internet.
- Generally blocks social networking sites except those that are part of an educational network or required specific educational purposes;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable
- Requires staff to preview websites before use.
- Never allows conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the online safety coordinator (head)
- 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;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

### 4.2 Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses 'remote' management control tools for controlling workstations / viewing users / setting-up applications where appropriate.
- Storage of all data within the school will conform to the UK data protection requirements.

*To ensure the network is used safely, this school:*

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Staff access to school systems is through a unique, audited username and password.

- Staff access to the schools' management information system (SIMS) is controlled through a separate password for data security purposes;
- Makes clear that no one should log on as another user
- Has set-up the network with a shared work area for staff. Staff are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or lock computers if leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that staff shutdown computers when they have finished using them. That computers in the class are not switched off during the day unless they are unlikely to be used again that day or have completely crashed. We require that all computers are shutdown the computers off at the end of the day.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring 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.
- Maintains equipment to ensure Health and Safety is followed; e.g. equipment installed and checked by approved Suppliers and electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEND coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support,
- Has a clear disaster recovery system in place
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

### 4.3 Password policy

- This school makes it clear that staff must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- We require staff to change their network passwords every 60 days .

### 4.4 E-mail

**This school**

- Provides staff with an email account for their professional use
- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / for communication with the wider public.
- Will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the school, including a desktop anti-virus product plus direct email filtering for viruses, Trojans, phishing and inappropriate language.

**Pupils:**

- Pupils currently have no unsupervised access to the internet at school.

**Staff:**

- access in school to external personal e mail accounts may be blocked
- use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- must only send personal data if sanctioned by the headteacher and this data must be encrypted
- know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;
- sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

### 4.5 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, admin@margaretmcmillan.islington.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images

### 4.6 Social networking

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

### 4.7 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. Recordings are subject to data protection legislation.

## 5. Data security: Management Information System access and Data transfer

### 5.1 Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record spreadsheet.
- We ensure ALL stakeholders are aware of and abide by an Acceptable Use Agreement form.
- This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- We are aware of our statutory responsibilities under GDPR and work within the current legislation.

### 5.2 Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use a 2-factor authentication for remote access into our systems.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Any back up tape taken off-site is encrypted.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data is disposed of through the same procedure.
- Paper based sensitive information is shredded or burnt.

## 6. Equipment and Digital Content

### 6.1 Outside Users

Islington Adult and Community Learning use tablet devices via a network segregated from the wider school network. Visitors, such as outside trainers, therapists, CC partners, can access the internet via the school network with a designated login.

### 6.2 Personal mobile phones and mobile devices

- Designated ‘mobile use free’ areas are situated in the setting, and signs are to be displayed throughout. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site.
- We require ACL not to give out wireless keys to individuals but to configure their devices themselves.
- We require all network users to abide by an Acceptable Use Policy agreement.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- If staff need to be contacted during the school day, they should do so only through the School’s telephone. Staff may use their phones during break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. Mobile phones should be kept in staff lockers and should be switched off or silent at all times.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

- All individuals who bring a mobile device into the setting must ensure they hold no inappropriate or illegal content.

### 6.3 Staff use of personal devices

- Staff do not use personal devices in school.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff have access to a school phone where contact with parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- All individuals who bring a mobile device into the setting must ensure they hold no inappropriate or illegal content

### 6.4 Digital images and video

**In this school:**

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use

### 6.5 Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

| | |
|---|---|
| Date reviewed | October 2025 |
| Date of next review | October 2027 |
| Ratified by Governing Body | October 2022 |