School E-Safety & Acceptable Use Policy

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

At our school the responsibility of e-safety is shared between the Headteacher, Designated Safeguarding Lead and the Computing Lead.
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.

Updated October 2023

1. Introduction and Overview

- **Rationale:**

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Millfields with respect to the use of ICT-based technologies;
- Safeguard and protect the children and staff of our 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;
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies;
- 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.

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 (including '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)

Communication:

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

- Policy to be posted on the school website/staffroom/ classrooms;
- Policy to be emailed to parents with AUP to be signed
- Policy to be part of school induction pack for new staff;
- Acceptable use agreements discussed with pupils at the start of each year;
- Acceptable use agreements to be issued to whole school community, usually on entry to the school;
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety including security filters and firewalls. 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 always 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 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, including examination coursework;
  - Referral to LA / Police.
  - Our E-safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher;
  - Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring:

The E-safety & Acceptable Use Policy should be reviewed in conjunction with the following policies:

- Anti-Bullying Policy;
- Safeguarding Policy;
- Positive Behaviour Management Policy;
- Social Media Policy;
- Asset Management Policy;
- FOI & Data Protection Policy;

The school has an E-safety Coordinator who will be responsible for document ownership, review and updates.

The E-safety & Acceptable Use Policy will be reviewed every three years or when any significant changes occur with regard to the technologies in use within the school.

The E-safety & Acceptable Use Policy has been written by the school Computing Lead /E-safety Lead, and has been reviewed by governors and is current and appropriate for its intended audience and purpose.

2. Education and Curriculum

- **Pupil e-safety curriculum:**
  The school:
  - Has a clear, progressive e-safety education programme. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK;
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - To be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - To know how to narrow down or refine a search;
    - (For older pupils) To understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;

- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- (For older pupils) To understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying; To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as CHILDLINE or the CLICK CEOP button.
- Use internet plans carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through Appendices 3 & 4;
- 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 and pupils 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 commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

- **Staff and governor training:**
  This school:
  - Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt 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 updates/ termly staff meetings etc.
- **Parent awareness and training:**
  This school runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear;
  - Information leaflets; in school newsletters; on the school website;
  - Demonstrations, practical sessions held at school;
  - Suggestions for safe Internet use at home;
  - Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

- **Expected conduct:**
  In this school, all users:
  - Are responsible for using the school ICT systems in accordance with this policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils);
  - Need to understand the importance 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 & Acceptable Use 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 handheld 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 E-safety & Acceptable Use Policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices.

Students/Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- **Parents/Carers:**
  - Should read, understand and sign the Parents AUP (Acceptable use Policy)
  - Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
  - Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

- **Incident Management:**
  In this school:
  - There is strict monitoring and application of the E-safety & Acceptable Use 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 authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues;
  - Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. A working group involving leadership, DSLs and our IT team meet periodically where records are reviewed/audited and reported to the school's senior leaders, Governors /the LA;
  - 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. Refer to Appendix 2.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering:**
  This school:
  - Uses a secure firewall, which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to approved staff.
  - Uses device-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
  - Ensures network healthy through use of Anti-Virus and network set-up so staff and pupils cannot download executable files;
  - Uses DfE approved systems such as S2S and secured email to send personal data over the Internet and uses encrypted devices and secure remote access were staff need to access personal level data off-site;
  - Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
  - Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
  - Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
  - Uses security time-outs on Internet access where practicable / useful;
  - Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
  - Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;

- Ensures pupils only publish within an appropriately secure environment : the school's website and the school's online learning environment google classroom;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate websites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg Google Safe Search; Best practice states that it is important that staff are able to a) demonstrate this b) they quote this practice if they are asked at any time
- Is vigilant when 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 IT Coordinator to be escalated to the system administrator
- 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.

The DfE has published guidance for Headteachers, school staff and governing bodies in terms of searching, screening and confiscation. Please visit DfE - Searching, screening and confiscation.

- **Network management (user access, backup):**
  This school:
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
  - Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
  - Storage of all confidential data within the school will conform to the UK data protection requirements;
  - Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

- **To ensure the network is used safely**;
  This school:
  - Ensures staff read and sign that they have understood the school's E-safety & Acceptable Use Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
  - Staff access to the schools' management information system is controlled through a separate password for data security purposes;
  - Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
  - Provides each student with a unique username and password to sign in to Chromebooks, which restricts traffic where appropriate based on OUs defined with Google Admin, as approved by leadership and systems administrators
  - Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils 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 are 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 teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day; unless they plan on working remotely
  - Has set-up the network so that users cannot download executable files / programmes;
  - 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;

- Installs Anti-Virus on any devices approved for removal from the domain environment, as well as SSID filtering as required to protect other devices not approved for removal.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc;
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager; equipment installed and checked by approved Suppliers / LA 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; SEN 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 / LA approved systems (e.g. Google Drive or configured and authenticated RDS servers / OpenVPN remote access)
- 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), our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back-up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back-up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure S2S website for all CTF files sent to other schools;
- Ensures 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
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /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 with regard to health and safety and security, with a working group composed of leadership, DSL and IT meeting regularly.

- **Passwords policy:**
  - This school makes it clear that staff keep their password private, must not share it with others and must not leave it where others can find;
  - 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 for information on data management please refer to the Records Management Policy.

- **E-mail:**
  This school:
  - Provides staff with an email account for their professional use using Google Mail, and makes clear personal email should be through a separate account;
  - Does not publish personal email addresses of pupils or staff on the school website. We use anonymous or group email addresses, for example info@millfields.hackney.sch.uk for communication with the wider public;
  - Will contact the Police if one of our staff or pupils receives an email 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 desktop anti-virus product Kaspersky, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, the school's firewall filtering monitors and protects our internet access to the World Wide Web;

- In accordance with the Data Protection Act 1998 the school reserves the right to monitor the use of these systems. Emails may be inspected at any time without notice where malpractice is suspected;

- **Pupils:**
  - Each student is provided with a unique username and password, with which the are expected to use Chromebooks for any work requiring access to the network or shared files, folders and/or documents
  - Pupils' are not allowed email accounts
  - Pupils are introduced to, and use email as part of the Computing scheme of work within a secure and isolated environment solely for the purpose of demonstrating this;
  - Pupils are taught about the safety and 'netiquette' of using e-mail both in a professional setting and at home i.e. they are taught:
    - Not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - That any email communications should be written carefully and with consideration to the content contained within these
    - That any email should only contain details relevant to the recipient and that the sharing of confidential or protected details, files or information should only be distributed to those to whom authorization has been granted to share this information with
    - They must not reveal private details of themselves or others in email, such as address, telephone number, etc;
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - That they should think carefully before sending any attachments;
    - Embedding adverts is not allowed;
    - That they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
    - Not to respond to malicious or threatening messages;
    - Not to delete malicious of threatening emails, but to keep them as evidence of bullying;
    - Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - That forwarding 'chain' e-mail letters is not permitted.
  - Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with. See Appendix 1.

- **Staff:**
  - Staff can only use the school e-mail systems on the school system;
  - Staff only use school email systems for professional purposes;
  - Access in school to external personal email accounts may be blocked;
  - The school utilise a secure 'managed' email domain for all communications via a cloud-based SAAS system with admin level-oversight delegated to system administrators and the School Business Manager for separation of privileges
  - Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA system;
  - Staff know that email 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;
    - All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

- **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 website 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, e.g. info@millfields.hackney.sch.uk . Home information or individual email 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 geo data in respect of stored images;
    - We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

- **Social networking:**
    - Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications;
    - The school's preferred system for social networking will be maintained in adherence with the Social Media Policy.

- **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.

- **Video Conferencing:**
  This school only uses DfE approved or checked webcam sites.

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

- **Strategic and operational practices:**
  Please refer to the Records Management Policy and for more information in managing student data and Remote Back-Up Policy.

- **Technical Solutions:**
    - Staff have secure areas on the network to store sensitive documents or photographs.
    - We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
    - We use HTTPS encrypted Windows RDS servers or Untangle's OpenVPN for remote access into our systems, configured via user and/or group policy to restrict access to only authorised users of these solutions
    - We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
    - All servers are in lockable locations and managed by DBS-checked staff.
    - We use Turn IT On's NAS Discover backup for on-site disaster recovery on our servers.
    - We use Redstor for off-site backup storage of key/sensitive data
    - 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 out 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, using cross cut shredder / collected by secure data disposal service.

6. Equipment and Digital Content

- **Personal mobile phones and mobile devices:**
  - Mobile phones brought into school are entirely at the staff member, students & parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school;
  - Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times;
  - All visitors are requested to keep their phones on silent and not use the phone around the school;
  - The recording, taking and sharing of images, video and audio on any personal mobile phone is not permitted;
  - The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying;
  - Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times;
  - Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times and not accessed in the school or where pupils are present;
  - Personally-owned mobile devices should only be connected to the 'Millfields Guest' WiFi SSID, with the password available to visitors on request
  -
  - Mobile phones will not be used unless directed by the Headteacher for specific purposes (e.g. method of contact on a school trip);
  - 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 mobile phones and personally-owned devices will be handed in at reception should they be brought into school;
  - The exception to the above rules are phones that belong to the school and are provided for business use. All work phones are subject to random review and inspection.

- **Students' use of personal devices:**
  - The School strongly advises that student mobile phones should not be brought into school;
  - The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety;
  - If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy;
  - Phones and devices must be handed to the school office at the beginning of each day;
  - If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;
  - Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences;
  - Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled;
  - Any device brought into school and used in breach of this policy will be confiscated.

- **Staff use of personal devices:**
    - Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day;
    - 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 will be issued with a school phone where contact with students, parents or carers is required;
    - Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode;
    - 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 students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't 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.

- **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;
    - If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use;
    - The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
    - Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
    - Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
    - Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

- **Recording of plays and events – Parents:**
    - Please see the appendices section for the school's guidance on recording of plays and events for parents.

- **Asset disposal:**
    - Please refer to the school's Asset Disposal Policy

APPENDIX 1 – Acceptable use agreement for staff

Acceptable Use Agreement
STAFF

Introduction

This document has been developed to ensure all staff at Millfields Community School are aware of their professional responsibilities when using ICT equipment and systems. All staff will follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home or on school visits. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage. When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the E-Safety Officer and/or the Headteacher.
- I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords with any colleagues or pupils within school.
- I will seek consent from the E-Safety Officer / Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the E-Safety Officer / Headteacher
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the E-Safety Officer / Headteacher / Systems Administrator at the earliest opportunity
- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site. I will also sign a declaration form that states that the device is my responsibility prior to taking it off site.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will secure any equipment taken off site for school trips.
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed. I will not use any other portable storage device on the school network as I understand this carries risks to the security of the network.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance

with the school data protection. (For example spreadsheets/other documents created from information located within the school information management system).

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the eSafety Officer / Headteacher
- I will return any school-owned ICT equipment or software to the relevant individual within school (ICT Consultant) once it is no longer required or/and when requested by the ICT Consultant or the Headteacher.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the school's established disciplinary procedures.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I must obtain permission from the Headteacher if I wish to use social media with pupils for educational purposes.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the eSafety Officer / Headteacher.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the pupils involved and in line with the e-safety policy.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff. (eSafety officer/ Headteacher).
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and teaching

- I will support and promote the school eSafety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.

- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

- I will use my school email address for all correspondence with staff or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and members of the wider school community should be professional and related to school matters only.
- I must not communicate with parents using any digital media other than my school email address.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will not synchronise any school email account with a personally-owned handheld device, unless adequate additional security features have been enabled to protect against access (e.g. device-level encryption, passwords and/or passcodes).
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the headteacher, phase leader or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to ‘silent’ mode during school hours.
- Bluetooth communication will be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not connect any mobile device to the schools wireless network at any time
- I will not connect any mobile device to the school network at any time
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings

I have read and understand all of the Millfields Community Primary School Staff and Volunteer Acceptable Use Policy relating to my use of technology. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff name

Signed

Date

APPENDIX 2 – Acceptable use agreement for parents

Acceptable Use Agreement
PARENTS

What is an Acceptable Use Agreement

We ask all children, young people and adults involved in the life of Millfields Community School to sign an Acceptable Use Policy, which is a document that outlines how we expect them to **behave when they are online**, and/or **using school networks**, **connections, internet connectivity and devices, cloud platforms such as ' Google Classroom' and social media** (both when on school site and outside of school).
Your child/ren will also sign an AUP at Millfields Community School.

Why do we need an AUP?
These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.
School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.
We tell your child/ren how to behave online, and that they should not behave any differently when they are not in school or using their own device at home or on a home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read Millfield's full Online Safety Policy on the school www.millfields.hackney.sch.uk for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please email your comments to info@millfields.hackney.sch.uk

What am I agreeing to?

1. I understand that Millfields Community School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. School policies and agreements are in place to keep your children safe including web filters, firewalls and specific policies. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies that may occasionally bypass security systems.

3. I understand that internet and devices used in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media safeguarding protocols and not encourage my child to join any platform where they are below the minimum age.

6. I will follow the school's digital images and video procedures, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous.

7. I understand that the school sometimes uses images/video of my child for internal communications and attainment purposes such as assemblies and on the website. I will already have signed the consent form for this on my child's admission to the school.

8. I understand that for my child to be safe safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year).

9. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.

10. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day:

11. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which they have signed, and which can be seen obtained from our website: I understand that they will be subject to sanctions if they do not follow these rules.

12. I can find out more about online safety at Millfields by reading the full Online Safety Policy here and can talk to their class teacher or senior leaders at the school if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.
Signature/s: _____
Name/s of parent / guardian: _____
Parent / guardian of: _____
Date: _____

Please note that parents may also be interested in the school's approach to the following matters, which are all covered as sections within the overall school Online Safety Policy: Roles and responsibilities of members of the school community

- Education and curriculum
- Handling online-safety concerns and incidents
- Actions where there are concerns about a child
    - Sexting and upskirting
    - Bullying
    - Sexual violence and harassment
    - Misuse of school technology (devices, systems, networks or platforms)
    - Social media incidents
- Data protection and data security
- Appropriate filtering and monitoring
- Electronic communications
- Email
- School website
- Cloud platforms
- Digital images and video
- Social media
- Device usage
~~~~~~~~~~~~~~~~~~~~~

APPENDIX 3: - Acceptable use agreement for children in Key Stage 1

Acceptable Use Agreement
PUPILS

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I am stuck or not sure
3. I **TELL** a trusted adult if I am upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online are not always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep ~~**SECRETS**~~ or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

My trusted adults are:

_____ **at school**
_____ **at school**
_____ **at home**

APPENDIX 4 : - Acceptable use agreement for children in Key Stage 2

Acceptable Use Agreement
KS2 PUPILS

These statements can keep me and others safe & happy at school and home

I learn online – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

I learn even when I can't go to school because of coronavirus – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.

I ask permission – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

I am creative online – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.

I am a friend online – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.

I know new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

I check with a parent/carer before I meet an online friend the first time; I never go alone.

I don't do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

I keep my body to myself online – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

I say no online if I need to – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I follow age rules – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.

I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

I am a rule-follower online – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

I am not a bully – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

I am part of a community – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

I respect people's work – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

I am a researcher online – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

_____

Outside school, my trusted adults are_____

Signed: _____ Date: _____
~~~~~~~~~~~~~~~~~~~~

APPENDIX 6 – Guidance for parents taking photographs of events

We stage numerous school events and know some parents/carers like to take photographs/videos of the school productions. As you know we have a policy in place with regards to the taking, making and use of images and you will have previously signed a consent form stating whether or not your child could be photographed.

At Millfields, we are happy for parents and carers to take photos and video of events for personal use but we request that these images are not distributed or put online. This is to protect all members of the community.

If you wish to take photos at the production there is a strong possibility that other children will also be included within the picture. The Data Protection Act 1998 does not stop a person's image from being captured, but it does require the image to be obtained fairly, used for a legitimate purpose which does not cause the individual distress or prejudice and be kept securely.

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video. We now have the exciting dimension of adding our images and videos to our online social network, such as Facebook, YouTube and many other websites. This means that we can easily share our photos and videos with family and friends.

Whilst this can be very useful to all of us we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

Please be aware that parents are not permitted to take photographs or to make a video recording for anything other than their own personal use.

If you have any queries please speak to a member of the school leadership.

Generally photographs and videos for school and family use are a source of innocent pleasure and pride which can enhance self-esteem for children and young people and their families. By following some simple guidelines we can proceed safely and with regard to the law:

Remember that parents and carers attend school events at the invitation of the head and governors.

The head and governors have the responsibility to decide if photography and videoing of school performances is permitted.

The head and governors have the responsibility to decide the conditions that will apply in order that children are kept safe and that the performance is not disrupted and children and staff not distracted.

Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos cannot be sold and must not be put on the web/internet. This includes Facebook, Twitter, Instagram, Snapchat and other social media.

Recording or/photographing other than for private use would require the consent of all the other parents whose children may be included in the images.

Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

Parents and carers must not photograph or video children changing for performances or events.

If you are accompanied or represented by people that school staff do not recognise they may need to check out who they are if they are using a camera or video recorder.