MAYFIELD PREPARATORY SCHOOL

Believe It! Achieve It!

School E-Safety Policy

Content

1. Introduction and Overview

This policy applies to all pupils at Mayfield Preparatory School, including all pupils in the Early Years Foundation Stage.

Rationale

The purpose of this policy is:

- To set out the key principles expected of all members of the school community at Mayfield Preparatory School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Mayfield Preparatory 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
- Radicalisation
- 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

Scope
This policy applies to all members of Mayfield Preparatory School community, including in the Early Years Foundation Stage (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Mayfield Preparatory 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.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator • 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)
E-Safety Co-ordinator (Head of ICT)	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school ICT technical staff • To communicate regularly with SMT and the nominated Governor for Child Protection to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • To ensure that an e-Safety incident log is kept up to date • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • Sharing of personal data • Access to illegal / inappropriate materials • Inappropriate on-line contact with adults / strangers • Potential or actual incidents of grooming Cyber-bullying and use of social media
Governors and Nominated Governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports via the Headmaster. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the nominated Governor for Child Protection will include a regular review with the E-Safety Co-ordinator. (including E-safety incident logs, filtering / change control logs)
Head of ICT	• To oversee the delivery of the e-safety element of the ICT curriculum. • To liaise with the e-safety coordinator regularly

Role	Key Responsibilities
Network Manager School Technical Support (Concero)	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • 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. • To ensure that provision exists for misuse detection and malicious attack e.g. Keeping virus protection up to date. • To ensure the security of the school ICT system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and updated on a regular basis. • That he / she 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 That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager (Head of ICT)	To ensure that all data held on pupils on the school office machines have appropriate access controls in place
CONCERO (School ICT Support)	To ensure all services are managed on behalf of the school including maintaining the database of access accounts, Internet Access, Online Learning Environment Tools (Espresso) and the School Information Management System (SIMS)
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand and adhere to the school staff Acceptable Use Agreement / Policy • 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 • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • 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, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand and adhere to the Pupil Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. • To help the school in the creation/ review of e-safety policies
Parents/ Carers	• To support the school in promoting e-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 • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will read an Acceptable Use Policy prior to using any equipment or the internet within school

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/ available to parents
- 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 agreed by staff (including volunteers, work experience and visitors) and pupils on first entry into network each academic year

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 Internet Connection Provider (CONCERO) can accept liability for material accessed, or any consequences of Internet access.

If a parent wishes to make a formal complaint about issues related to this policy they should follow the school's complaints procedure.

A child's class Tutor or our E-Safety Coordinator act as first points 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 safeguarding procedures.

Review and Monitoring
The e-safety policy is referenced from within other school policies: ICT policy, Safeguarding policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

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

The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.

The Policy has been agreed by SMT and approved by the governors. Amendments to the policy will be discussed with all members of teaching staff.

2. Education and Curriculum
Pupil e-Safety curriculum
This school:
Has a clear, progressive e-safety education programme as part of the ICT curriculum / PSHE curriculum. It is built on e-Safeguarding and e-literacy guidance for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK – Maintain Control and Communicate if there is a concern
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / 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.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will read and will be displayed throughout the school. The school is looking at this information being displayed when a student logs on to the school network.
- 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; annual updates/ termly 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 e-safety Policy and the school's Acceptable Use Policies.

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 web site;
- 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
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 read before being given access to school systems.
- 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
- 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 e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.
Students/Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
Parents/Carers 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

<u>Incident Management</u>
In this school:

- There is strict monitoring and application of the e-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 (eg the local authority and regional, UK safer internet centre helpline, CEOP) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's Senior leaders, Governors, then if necessary to the local authority / 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
Internet access, security (virus protection) and filtering
This school:

- Has the educational filtered secure broadband connectivity through CONCERO, the school's ICT support service.
- The school uses the CONCERO Senso filtering system 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 is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-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 Symantec anti-virus software (from CONCERO) etc and network set-up so only approved staff and not pupils can download executable files;
- Uses approved systems for secured email to send personal data over the Internet and uses encrypted devices or 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 environment.
- 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, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with CONCERO to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- 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 read an acceptable use agreement form and understand that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's network as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search , …..
- Never allows / 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 Head of ICT who is also the school network system administrator. This will be logged and the Technical service provider or CONCERO Helpdesk will be contacted if necessary;

- 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.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users from Lower II to Lower III with pupils. Pupils below Lower II use class accounts. All staff have separate accounts.
- 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;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all 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 ensure that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to services is through a unique, audited username and password. We also provide a different username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Upper II they are also expected to use a personal password;
- All pupils have their own unique username from Lower II to Lower III and have a password which gives them access to the Internet, the school software *and (for older pupils) their own school approved email account*;
- 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;
- 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. [Users needing access to secure data are timed out after 10 mins and have to re-enter their username and password to re-enter the network].
- 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 and we also automatically switch off all computers at 9.30pm to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;

- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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 device 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. projector filters cleaned by site manager / TA; 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 / CONCERO approved systems: e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution;
- 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.
- Provides pupils and staff with access to content and resources through the school network or online learning area 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;
- 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 school or through an CONCERO approved system.
- Follows 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 and interactive panels are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

This school makes it clear that staff and pupils must always 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.

We require staff to change their passwords into the MIS and associated programs annually.

E-mail

This school

Provides staff with an email account for their professional use, and make clear personal email should be through a separate account;

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use e-mail addresses with specific school names, for example info@mayfieldprep.co.uk, staffname@mayfieldprep.co.uk or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.

- Will contact the Police if one of our staff or pupils 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 e mails dangerous.
- We use a number of CONCERO-provided technologies to help protect users and systems in the school, including desktop anti-virus product Symantec, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, Senso filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- When using email, pupils access 'anonymised' accounts ending @mayfieldprep.co.uk
- We use O365 as our email client and lock this down where appropriate using appropriate access rules.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- Kindergarten and transition pupils an pupils are introduced to principles of e-mail through a closed 'simulation' software.
- Pupils can only receive external mail from, and send external mail to, addresses if the email rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. They are taught:

    - Not to give out their e-mail 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 e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - They must not reveal private details of themselves or others in e-mail, 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 e-mail 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 e-mails, 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 will read the Acceptable Use policy and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can use the e-mail systems on the school system and via the internet by logging onto the O365 service.
- Staff only use school e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure VPN connections from devices to the school network. Information should be held within the school SIMS and accessed from here.

- Staff 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;
- All staff will read the Acceptable Use policy and understood the e-safety rules, including e-mail 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: Head of ICT, Headmaster, Deputy-Head and Network Manager;

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@mayfieldprep.co.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

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 house.

- 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.
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses CONCERO supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

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

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 (the Information Asset Owners) are.

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, the Single Central Register for Staff Appointments.

We ensure ALL the following school stakeholders read an Acceptable Use Agreement form.

- Staff, governors, pupils and parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

We follow LA guidelines for the transfer of any 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 undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- Laptops are bit-locker encrypted as are any mobile storage devices such as USBs or Portable Hard-drives.
- 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.
- Our backup service is managed by CONCERO services and is in an off-site secure server location. All back-ups are encrypted and no back-up leaves the site on mobile devices.
- We use CONCERO Services for disaster recovery on our network and servers.
- 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, using cross cut shredder.
- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

The school operates a separate mobile phone policy.
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. Any images of pupils recorded on personal mobile phones must be uploaded as soon as possible onto safe storage at school and deleted from the mobile phone. (see school policy on recording, taking and storing images of children).
The school reserves the right to search the content of electronic devices and deal with electronic devices in accordance with guidance issued by DfE "Searching, Screening and Confiscation" Advice for headteachers, school staff and governing bodies. February 2014.

Students' use of personal devices

- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Staff use of personal devices

- Staff will be issued with a school phone where contact with students, parents or carers is required.
- If members of staff have an educational reason to allow children to a personally-owned device as part of an educational activity then it will only take place when approved by the senior management team.
- 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.

Mobile Devices / BYOD

BYOD practice is not utilised at Mayfield as all devices to facilitate teaching/ learning/ administration/ support are provided by the school. Mobile phones are deemed safe to have the outlook app on them for email as accounts can be "force closed" (logged out) remotely through Concero if lost or stolen, it is advisable that it is only installed on phones that are pin locked.

Digital images and video

The school has a separate policy regarding 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 read the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
The school obtains parent/carer permission to use pupils' photographs on the website, in the prospectus or for promotional purposes. Parent/carers have the right to refuse permission and the school will respect their wishes.
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 eSafety 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 identify 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.

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.

Legislation
The legislative framework under which this E-Safety Policy and guidance has been produced is based on the advice and material available at the time of review. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the event of an e-safety issue or situation.

Reviewed: December 2022
Review Date: December 2024
Head of ICT: Emma Hawthorne
Headmaster: Matthew Draper
Chair of Governors: Simon Thacker

ASSOCIATED DOCUMENTS

Acceptable Usage Policy – Staff

This document has been written to ensure that staff use the ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Management team or the Head of ICT. Staff should:

- Use computers and equipment with care and ensure pupils do the same e.g. water bottles should stay away from machines.
- Ensure that they have a sensible password combining letters and numbers.
- Staff should have complex passwords, combining letters, special characters and numbers.
- Ensure that usernames and passwords are not shared with pupils or other staff.
- Ensure that they log off when they have finished using a computer – particularly in shared areas – or lock computer when away for a period of time, using Windows Key and L.
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files regularly.
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper.
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or pupils remains professional at all times.
- Ensure that online activity is related to their professional duty and that personal use should. be kept to a minimum and only outside of directed teaching time e.g. online personal shopping.
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites.
- Ensure that they have read and understood the ICT Policy.
- Be aware that software or hardware should not be installed without prior consent of the Head of ICT, Head teacher or Network Manager.
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Head teacher.
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under GDPR and is subject to the school's Data Protection Policy. **Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical**.
- Staff should not use their own digital equipment to take pictures.
- Report any issues to the Senior Management team or Head of ICT as soon as possible.
- Return any hardware or equipment if they are no longer employed by the school.

Members of Staff of Mayfield Preparatory School are expected to read and abide by all the school policies (see Staff Code of Conduct). If any members of staff have any queries regarding this policy, please contact the Head of ICT or a member of the Senior Management Team.

Acceptable Usage Policy Pupils

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, netbooks, and everything else including cameras and other devices. All pupils, including those pupils in the Early Years Foundation Stage, at Mayfield Preparatory School are expected to abide by the school rules. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher or Mrs Hawthorne.

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will tell my teacher straight away.
- When communicating online (in blogs, email etc.) I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not logon using another person's account.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will take care when using the computers and transporting equipment around.
- I will keep my usernames and passwords secure from persons outside Mayfield, but I understand I can share them with appropriate people, such as my parents or teachers.
- I will not install any software or hardware (including memory sticks) without permission from a teacher.
- I understand that if I am acting inappropriately then my parents may be informed.

Acceptable Usage Policy KS1 Pupils – Linked to 360Safe AUP Guidelines
These rules have been written to make sure that you stay safe when using the computers. This includes cameras, netbooks and microphones too. All pupils, including those pupils in the Early Years Foundation Stage, at Mayfield Preparatory School are expected to abide by the school rules. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules and a copy will be sent home to your parents.

If you have any questions, please ask your teacher or Mrs Hawthorne.

The Golden Rule: **Control and Communicate - Think before you click**

☺ I will be careful when going on the internet.
☺ I will only use the internet when a teacher is with me.
☺ I will tell a teacher if I see something that upsets me.
☺ I know people online might not be who they say they are.
☺ I will be polite when talking to people or writing online.
☺ I will think before I print or delete.
☺ I will be careful when using or carrying equipment.
☺ Remember to log off properly before closing the lid of the netbooks.
☹ I won't share personal details like my school, phone number or last name.
☹ I won't logon using someone else's username.
☹ Never put water bottles on the table when using the ICT room.

Acceptable Usage Policy - Parents

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- *That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.*

- *That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.*

- *That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.*

- *The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this form, so that parents / carers will be aware of the school expectations of the young people in their care.*

The school wishes to remind its parents that Facebook, Instagram and other Social Medias are only intended for users aged over 13, Whatsapp has a minimum age of 16. The school also understands that it is very easy for young people (or indeed adults) to enter an incorrect date of birth or false information to open an account. In fact, according to Ofcom's UK Media Literacy report "social networking continues to increase and 47% of 10 – 12 year olds have an active profile".

Concerns have been raised over some of the possible issues including:

- *Interactions between pupils, parents or staff.*
- *Inappropriate communications between users*
- *Unpleasant or abusive postings about teachers or pupils.*
- *Criticism of the school (not personally abusive).*
- *The setting up of fake profiles*

Any form of misuse directed at the school, its employees, the pupils or anyone associated with the school will be taken very seriously. The school will follow the anti-bullying, behaviour and discipline, sanctions and exclusion policies. If any illegal activity or content is suspected the school will inform the necessary authorities.

All pupils will have access to the internet and to ICT systems at school. As the parent of a pupil of Mayfield Preparatory School, it is understood that all pupils, parents, members of staff, governors and visitors to the school are expected to abide by all the school policies. If any members of staff have any queries regarding this policy, please contact the Head of ICT or a member of the Senior Management Team.

All pupils have received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school. The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

All pupils' activity on the ICT systems will be monitored and the school will contact parents if they have concerns about any possible breaches of the Acceptable Use Policy.

It is the parents' responsibility to encourage their child to adopt safe use of the internet and digital technologies at home and to inform the school if there are concerns over their child's e-safety.

Use of Office 365:

The school uses Office 365 for pupils / students and staff. The information below describes the tools and pupil/ student responsibilities for using these services. The services offered by Office 365 are to be used with the guidance of parents or teachers. They should also be used in accordance with the school AUP.

Acceptable Usage Policy Governors and Visitors – Linked to 360Safe AUP Guidelines

Visitors, both physical and virtual, may be provided with accounts to our network and/or online systems. Visitors will have a lower level of access than staff and each account will be provided on a case-by-case basis. This will depend on the purpose of the account requested.

School Network and wireless

Users will:

- Be given a login for their time in the school
- Be expected to follow the guidelines as set out for staff
- Understand that this account may be removed at any time
- Be provided with the wireless key and guidelines for connecting to the network

Governors and visitors to Mayfield Preparatory School are expected to abide by all the school policies). If any Governors or visitors have any queries regarding this policy, please contact the Head of ICT or a member of the Senior Management Team.