The Park Federation Academy Trust

Lake Farm Park Academy
E-Safety Policy

Approval

Approved by the Principal on behalf of the Academy Council	Craig Horsman
Date of approval	November 2015
Date of review	November 2017

Contents

Section 1: Overview

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety.

This policy covers the acceptable use of the Internet and related technologies. It has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and previous Becta guidance. It has been agreed by the senior leadership team and approved by the Academy Council

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Lake Farm Park Academy (LFPA) with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of LFPA.
- 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 potential risk 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)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

LFPA 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
Principal	• 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 e.g. LGfL • 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 / Officer • 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/ Designated Safeguarding Lead	• 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 SLT and the designated e-safety Governor / committee 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
Academy Council	• 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. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/ technician	• 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 • LGfL is informed of issues relating to the filtering applied by the Grid • that they keep 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 • 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
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
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, sign 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, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • 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 consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Communication

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use 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. 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 academy nor the Board of Directors 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:

- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA /Police.

Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal
Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with LFPA's Child Protection Policy and Procedures.

Review and Monitoring

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

There is widespread ownership of the policy and it has been agreed by the SLT and approved by the Academy Council. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Section 2: Education and Curriculum

The Curriculum

LFPA will have a clear, progressive e-safety education programme as part of the Computing and PSHE curriculums. This covers a range of skills and behaviours appropriate to their age and experience, including:

- Fostering a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaching pupils and informing staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or ICT Manager.
- Ensuring pupils and staff know what to do if there is a cyber-bullying incident;
- Ensuring all pupils know how to report any abuse;
- 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.

LFPA will:

- plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- ensure staff model safe and responsible behaviour in their own use of technology during lessons.
- ensure 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;
- ensure 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;
- 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;
- make regular training available to staff on e-safety issues, including an annual update.
- Provide ,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-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness

The academy will provide 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.

Section 3: Expected Conduct and Incident management

Expected conduct

At LFPA we expect that all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (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 Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

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

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

Incident Management

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 will be 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

The monitoring and reporting of any e-safety incidents will take place and contribute to developments in policy and practice in e-safety within the school.

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.

Section 4: Safe and Appropriate Use of the ICT infrastructure

Internet access, security (virus protection) and filtering

The academy:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper 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 Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, 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 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, such as Audio Network;
- Uses security time-outs on Internet access where practicable/useful;
- Works in partnership with the LGfL 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 signed an acceptable use agreement form and understands that they must report any concerns;
- 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 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; e.g. yahoo for kids, Google Safe Search
- 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 Principal.

- Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as 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.

LFPA 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 it; All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

Email

The academy:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- 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 LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

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 sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff should never use email to transfer staff or pupil personal data. We use secure DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX. All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- 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: lfpaoffice@theparkfederation.org. 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;
- The Principal takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is completed by our web designers ICYT Solutions, www.icytsolutions.co.uk. The calendar on our website is maintained by the Executive Assistant.
- The school web site complies with the school's guidelines for publications;

Social Media

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

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation. Please see the CCTV Policy for more information.

Section 5: Managing the ICT Network

The computer system and network is owned by the academy and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely the academy:

- Ensures staff read the E-safety Policy and signed and Acceptable Use (AUP) form. . Online access to service is through London Grid for Learning's Unified Sign-On (USO) system for usernames and passwords. We also provide a staff login and password for access to our school's network;
- Has separate curriculum and administration networks, for data security purposes;
- Staff access to the schools' management information system (SIMS) is controlled through a separate password for data security purposes;
- We provide pupils with a group/class network log-in username.
- 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;
- 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 (staff only) to lock their computer if they are leaving the computer temporarily unattended;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational or administrative 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 laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by technicians; equipment installed and checked by approved Suppliers / electrical engineers
- 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;
- 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 our broadband network for our CCTV system;
- 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 or through USO secure file exchange (USO FX);
- Provides staff with encrypted flash drive if they need to take any sensitive information off site.

- Uses the DfE S2S site to securely transfer CTF pupil data files to other schools.
- Uses the Pan-London Admissions system (based on USO FX) to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- Ensures all servers are in lockable locations and managed by DBS-checked staff.
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to health and safety and security.
- Uses Google's encrypted GMail to send personal data over the Internet and uses encrypted devices, encrypted Google Drive or secure remote access where 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;
- Only uses the Sisco Secure Switch service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Uses GMail provided by Google with pupils as this has email content control and the address does not identify the student or school;
- Provides staff with an email account for their professional use, GMail provided by Google and makes clear personal email should be through a separate account;
- Works in partnership with the LGfL/HGfL and Google to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Network Manager is up-to-date with LGfL, HGfL and Google services and policies / requires the Technical Support Provider to be up-to-date with LGfL and HGfL services and policies.

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 on an Excel spreadsheet.

Section 6: Equipment and Digital Content

The purpose of this policy is to prevent unacceptable use of mobile phones and other hand held devices by the school community, and thereby to protect the academy's staff and students from undesirable materials, filming, intimidation or harassment.

This section of the policy sets out what is 'acceptable' and 'unacceptable' use of mobile phone and handheld devices by the whole school community (students, staff and visitors) while they are at School or undertaking school activities away from school.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils' & parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- 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.

- 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.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting 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 'hide' their own mobile number for confidentiality purposes, using their Caller ID settings, or adding "141" before the number to be dialled.

Digital images and video

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

Responsible Internet Use
Parental Agreement

Please complete, sign and return to your child's class teacher

Pupil Name: _____ Class: _____

Parent's Consent for Internet Access and Use of Email
(email address given from Year 2 and above)

I have read and understand the school rules for Responsible Internet Use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials, while staff will employ appropriate teaching practice and teach e-safety skills to pupils. I understand that my child's teacher will review these rules and ask each child in the class to sign a class agreement to adhere to them (from Year 2 onwards). I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Signed: _____ Date: _____

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Responsible Internet Use
Pupil Agreement

Class: _____ Academic Year: _____

I have understand the school rules on using the computers and internet responsibly.

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Signed: _____ Date: _____

Responsible Internet Use
Pupil Agreement

We use the school computers and internet for learning.
These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved that site.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not look at or delete other people's files.
- I will keep my logins and passwords secret.
- I will only email people I know, or whom my teacher has approved.
- I will ask for permission before opening an email or an email attachment sent by someone I do not know.
- The messages I send will be polite and sensible.
- I will not give my home address, phone number, send a photograph or video, or give any personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or my email address.

Acceptable Use Policy
Staff Agreement Form

This policy covers the acceptable use of digital technologies used by school staff: i.e. email, internet, intranet (school network) and network resources**,** software, equipment, learning platform and systems.

- I will only use the academy's and Local Authority's (LA) digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the school and Academy Council, and in accordance with policies.
- I will not reveal my passwords to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email, Internet, intranet, network or other school or LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will only use the approved, secure email system or other school-approved communication systems for school business.
- I will only use the approved, secure email system or other school approved communication systems with pupils or parents/carers, and only for school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate ICT Manager.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any online activity, such as social networking sites, blogs etc, that I create or actively contribute to, do not compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff or named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

One copy is to be retained by member of staff/second copy for school file