Wood End Park Academy

eSafety Policy

Approval

Approved by the Principal on behalf of the Academy Council	Surjeet Johra
Date of approval	September 2015
Date of review	September 2017

Notes on Document Control

This document is the property of The Park Federation Academy Trust and its contents are confidential. It must not be reproduced, loaned or passed to a 3rd party without the permission of the authoriser.

It is controlled within the Park Federation Academy Trust Admin Server where the electronic master is held and can be accessed on a read only basis, subject to security permissions.

Users of the document are responsible for ensuring that they are working with the current version.

Paper or electronic copies may be taken for remote working etc. However, all paper copies or electronic copies not held within the Admin Server are uncontrolled.
Hence the footer 'DOCUMENT UNCONTROLLED WHEN PRINTED' which must not be changed.

Once issued, as a minimum this document shall be reviewed on an annual basis by the originating team/function. Any amendments shall be identified by a vertical line adjacent to the right hand margin.

To enable continuous improvement, all readers encouraged to notify the author of errors, omissions and any other form of feedback.

Contents

Section 1: Overview

This e-safety 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 Academy Council Governors.

1.1 Context

Harnessing Technology: Transforming learning and children's services [1] sets out the government plans for taking a strategic approach to the future development of Computing.
"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper Every Child Matters[2] and the provisions of the Children Act 2004[3], Working Together to Safeguard Children[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use Computing in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that Computing can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. Moreover, it can be used to promote radicalisation, extreme views and terrorism.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

---

[1] http://www.dfes.gov.uk/publications/e-strategy/

[2] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3] See Every Child Matters website [http://www.everychildmatters.gov.uk]

[4] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

1.2 The technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (e.g. http://www.msn.com) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (e.g. www.myspace.com / www.bebo.com / http://www.hi5.com / www.clubpenguin.com / http:www.facebook.com)
- Video broadcasting sites (e.g. http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com)
- Gaming Sites (e.g. http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with mobile internet and apps.
- Mobile tablet devices (e.g. iPad, Google Nexus, Kindle)
- Gaming Consoles (e.g. Xbox, Play Station3) with internet connection.

1.3 Whole school approach to the safe use of Computing

Creating a safe Computing learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.

1.4 Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school. The Principal ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the Computing team.

Our e-Safety team ensures they keep up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP)[5]. The school's e-Safety team ensures the Principal, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our Governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

1.5 Communications: Sharing the Policy

How will the policy be shared with pupils?

In Assembly:
E-Safety topics are covered in both KS1 and KS2 assemblies each year, including the annual Safer Internet Day led by the UK Safer Internet Day Centre www.saferinternet.org.uk, with follow up class based activities.

In Computing lessons:
Within the Computing curriculum, pupils are taught and reminded about e-safety during appropriate units, such as using email and online research. Instruction in responsible and safe use should precede Internet access. This approach also applies to cross-curricular lessons, where Computing (such as laptops or tablet computers with an internet connection) is used to support learning in other subjects.

In Class:
At the start of each academic year, pupils are introduced or reminded about the school's rules for responsible use of the internet. Class teachers encourage discussion of these rules, to ensure understanding, before all pupils sign a class agreement.

In all approaches, pupils are taught appropriate online behaviour, made aware of possible risks, taught to minimise these risks and reminded how to report a problem.

[5] http://www.ceop.gov.uk/

How will the policy be shared with staff?

Computing use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Staff training in safe and responsible Internet use and on the school's e-Safety Policy will be provided as required, allowing time for discussion of the issues and develop appropriate teaching strategies.

Induction of new staff should include a discussion of the school's e-Safety Policy.

All staff are required to read and sign an Acceptable Use (AUP) form, following training on the school's e-Safety Policy. The Principal will give authorisation for each new member of staff to be allowed access to an email account; be connected to the Intranet and Internet; and be able to use the school's Computing resources and systems.

How will the policy be shared with parents?

For all new pupils, parents are required to read the pupils' rules of Acceptable Use (AUP) and sign a Parental Agreement form before pupils are allowed access to the internet. Here parents agree to support the school by promoting safe use of the Internet and digital technology at home and will inform the school if they have any concerns over their child's e-safety.

Internet use in pupils' homes is increasing rapidly, and unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. As a result, the school will communicate additional safety information to parents. This may include: articles in the school newsletter; useful information and web links on the school website; or presentations to parents.

1.6 How will complaints regarding e-Safety be handled?

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 Park Federation Academy Trust can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / Head of Year / e-Safety team / Principal;
- 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 relating to child protection are dealt with in accordance with school child protection procedures.

The e-Safety team will keep a record of issues relating to pupil misuse of email or internet services.

Section 2: Managing the Internet Safely

2.1 Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through the HGfL / LGfL and so connects to the 'private' National Education Network;
- Uses the HGfL / LGfL 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 HGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all users on the Admin Network, and group logins for the Curriculum Network;
- 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;

2.2 Policy and procedures:

This school:

- 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;
- Requires staff to preview websites before use. 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 or ask for kids
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the class teacher / Computing Co-ordinator. Our Network Manager logs or escalates as appropriate to the Technical service provider or HGfL (Atomwide) as necessary;
- Requires pupils to individually sign an Acceptable Use (AUP) agreement form which is fully explained and used as part of the teaching programme, and pupils are taught to report any concerns.
- Requires all staff to sign an Acceptable Use (AUP) agreement form and keeps a copy on file;
- Ensures parents provide consent for pupils to use the Internet, as well as other Computing technologies, as part of the e-safety Acceptable Use (AUP) agreement form at time of their child's entry to the school;
- 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;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides E-safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities (e.g. Police).

2.3 Education and training

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Computing Co-ordinator.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to understand 'Netiquette' 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 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;
- 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 observe and respect 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;
- 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 training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents.

Section 3: Managing e-mail

3.1 Managing e-mail across the School

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group 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 disturbing or breaks the law.
- Manages accounts effectively with up to date account details of users.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of HGfL / 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. Finally, and in support of these, Lightspeed filtering monitors and protects our internet access to the World Wide Web.

3.2 Managing e-mail used by Pupils:

- Pupils' e-mail accounts (GMail provided by Google) are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- 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 e-safety Acceptable Use (AUP) 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.

3.3 Managing e-mail used by Staff:

- Staff can only use the Federation e-mail systems on the school system
- Staff only use Federation e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Ensure all personal data transferred is encrypted.
- 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;
- All staff sign our e-safety Acceptable Use Policy (AUP) 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.

Section 4: Use of digital and video images

4.1 Using digital and video images in school

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy (AUP) and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- 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 Computing 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.

4.2 Using digital and video images on 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;
- 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. 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.

4.3 Using CCTV

Refer to Park Federation Academy Trust CCTV Policy.

Section 5: Managing the Network and Equipment
General guidance for using the school network, equipment and data safely

The computer system / network is owned by the school 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 this school:

- Ensures staff read the school's e-safety Policy and signed and Acceptable Use (AUP) form. Following this, they are set-up with Internet, email access and network access. 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.
- All pupils have their own unique username and password which gives them access to the their own school approved email account (from Year 2) and some web-based services;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- 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;
- The network is programmed to automatically switch off all computers at 8 o'clock pm to save energy;
- 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.

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by 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 and have had set-up by approved partners;
- 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);
- 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;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- Reviews the school Computing systems regularly with regard to health and safety and security.

Section 6: Handheld Devices and mobile phones

6.1 Overview

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.

This applies to all individuals who have access to personal and/or work-related handheld devices within the broadest context of the setting. It includes children and young people, parents and carers, practitioners, managers, volunteers, students, governors, visitors, contractors and community users. This list is not exhaustive.

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

It must be understood that should handheld devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones and handheld devices can also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

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

6.2 Whole school use of handheld devices and mobile phones

- 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.
- Mobile phones will not be used during lessons or formal school time.
- All visitors are requested to keep their phones on silent.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- The Bluetooth function should be set to 'hidden' or switched off on a mobile phone and not be used to send images or files to other mobile phones.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

6.3 Pupils' use of handheld devices and mobile phones

- The School strongly advises that pupil mobile phones should not be brought into school. However, the School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- All pupils' mobile phones and personally-owned devices will be handed in at reception should they be brought into school, and collected at the end of the school day.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

6.4 Staff use of handheld devices and mobile phones

- 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.

Wood End Park Academy
Responsible Internet Use
Parental Agreement

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

Parent / guardian name: _____

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. 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: _____

Parent's Consent for Web Publication of Work, Photographs and Videos

I agree that, if selected, my son/daughter's work may be published on the school website. I also agree that photographs and videos that include my son/daughter may be published subject to the school rules that photographs and videos will not clearly identify individuals and that full names will not be used.

Signed: _____ Date: _____

Wood End Park Academy

Responsible Internet Use

Pupil's Agreement

Class:_____ Academic Year: _____

I have read and understand the school rules on Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

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: _____

Signed: _____ Date: _____

Wood End Park Academy

Responsible Internet Use

Pupil's Agreement

We use the school computers and Internet connection 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.

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.

Wood End Park Academy
Acceptable Use Policy (AUP) – 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 school's and Local Authority's (LA) digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body, 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 (currently: Atomwide SurgeMail, provided by Hillingdon Grid for Learning), school Learning Platform 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 Computing Co-ordinator.
- 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 Computing '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.

Acceptable Use Policy (AUP) – Staff agreement form

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 Computing resources and systems.

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

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature

I approve this user to be set-up.

Signature .... Date .....

Full Name ..... (printed)

One copy is to be retained by member of staff | Second copy for school file