HOLLY PARK
PRIMARY SCHOOL

Holly Park School
Online safety Policy

School Online Safety Co-ordinators	**Dominic Carini & Lewis Turner**
School Designated Teacher for safeguarding	**Maria Michael**
School named Governor for safeguarding	**Clare Wischhusen**
Online Safety Governor	

Our Online-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and will be approved by Governors. It will be reviewed annually.

Contents

This policy links with the UN Rights of the Child

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Holly Park School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Holly Park 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 and misogynist language and scenarios), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- Exposure to websites connected to radicalisation and extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- grooming for radicalisation
- online-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

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

Scope of the Policy

This policy applies to all members of the *school* (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 the *school*.

The Education and Inspections Act 2006 empowers Headteachers 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 school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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.

Context

Ofsted: A good school 'integrates issues about safety and safeguarding into the curriculum so that pupils have a strong understanding of how to keep themselves safe. The school is pro-active in building on collaborative working with other key agencies to reduce the risk of harm to pupils.'

Working towards ICT Mark

1c-4 Safeguarding
The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure.
There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

3b-2 Effective and safe use of digital resources
Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

Harnessing Technology: Transforming learning and children's services [1] sets out the government plans for taking a strategic approach to the future development of ICT.

"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 *Working Together to Safeguard Children*[2] 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 ICT 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 ICT 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.

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.

The Technologies

ICT 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 (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams

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

[2] 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]

- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.facebook.com , www.myspace.com / www.piczo.com / www.bebo.com , snap chat, Instagram, Twitter, TikTok)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.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
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Apps

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements:

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

Ref: Becta - E-safety Developing whole-school policies to support effective practice [3]

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for Online-Safety has been designated to a member of the school improvement team alongside our designated teacher for safeguarding.

Our school **Online Safety Co-ordinator** is the Key Leader for Innovations and New Technologies. At present Lewis Turner and Dominic Carini
Our **designated teacher** is Sally Thomas
Our **Safeguarding Governor** is Clare Wischhusen
Our **Online-Safety Governor** is Fiona Quinton
Our e-Safety Coordinator ensures they keep up to date with online -Safety issues and guidance through liaison with the Local Authority Online-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[4]. The school's Online-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

The following section outlines the online -safety roles and responsibilities of individuals and groups within the school:

Governors:

[3] http://schools.becta.org.uk/index.php?section=is
[4] http://www.ceop.gov.uk/

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

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Safeguarding Governor and another is the Online Safety Governor*. The role of the Online Safety *Governor* will include:

- *monitoring of online safety incident logs held by the Deputy Head*
- *reporting to relevant Governors / committee / meeting*

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community**
- **The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.**
- *The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online-safety roles and to train other colleagues, as relevant.*
- *The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*

Online Safety Coordinator:

- leads on online safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online -safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future online-safety developments,
- reports to *governors* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

ICT Technician:

The ICT technician is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required e-safety technical requirements and any *Local Authority / other relevant body* Online-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**

- *the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online-safety technical information in order to effectively carry out their online-safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher / Principal / Senior Leader; Online -Safety Coordinator*

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices 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; eBullying / Cyberbullying procedures

- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher* for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

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

If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's Online -Safety Policy.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential

Staff are reminded / updated about Online-Safety matters at least once a year. We have a whole school focus on e-safety annually during Anti-bullying week in November.

Child Protection / Safeguarding Designated Person

should be trained in Online -safety issues and be aware of the potential for serious child protection / safeguarding 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
- radicalisation and extremism
- cyber-bullying

Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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

Many pupils are very familiar with the culture of new technologies. Pupils' perceptions of the risks may not be mature; the e-safety rules will need to be explained or discussed.

Online-safety should be taught in all year groups, covering age-appropriate issues. Useful online-safety programmes include:

- Barnet and LGfL e-Safety and online-literacy Framework for EYFS-Y6 (www. safety.lgfl.net)
- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent sessions with demonstrations and suggestions for safe home Internet use.

Community Users

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – pupils - Online -Safety curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* / *pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Online-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- 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 web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- [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 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 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 sign/will be displayed throughout the school/will be 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.
- *Students / pupils should be helped to understand the need for and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. However particularly in upper KS2 teachers will want pupils to develop as discerning and responsible users of the Internet and to use their self managing skills, so they will support children in learning how to use search engines for themselves carefully – e.g typing in 'for kids' at the end of a search, looking for familiar sites e.g BBC*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, website,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns eg Safer Internet Day, Anti Bullying Week*
- *Reference to the relevant web sites / publications*

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online-safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive online-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- *The Online-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*

- *This Online-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Governors

Governors should take part in online-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff
  - There should be a governor with the specific role of Safeguarding and one for Online-safety

Extremism & Radicalisation

As part of Holly Park's commitment to safeguarding and child protection we fully support the government's *Prevent Strategy.*
The Prevent strategy is a government strategy designed to stop people becoming terrorists or supporting terrorism. It:

- responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views
- provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support
- works with a wide range of sectors (including education, criminal justice, faith, charities, online and health)

As part of our safeguarding ethos we encourage pupils to respect the fundamental British values of democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs. We ensure that partisan political views are not promoted in the teaching of any subject in the school and where political issues are brought to the attention of the pupils, reasonably practicable steps have been taken to offer a balanced presentation of opposing views to pupils.

Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.

Extremism is defined as the holding of extreme political or religious views.

There are a number of behaviours which may indicate a child is at risk of being radicalised or exposed to extreme views. These include several ways but in relation to this policy:

- Communications with others that suggests identification with a group, cause or ideology.
- Talking about internet activity and websites that may involve radicalisation

Although incidents involving radicalisation have not occurred at Holly Park School to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the local area, city and society in which we teach. Staff are reminded to suspend any 'professional disbelief' that instances of radicalisation 'could not happen here' and to be

'professionally inquisitive' where concerns arise, referring any concerns through the appropriate channels.

In Implementing the Prevent Duty at Holly Park we:
Try to keep up to date with online safety and share this with pupils, staff and parents.
Recognise and are aware of the part that an online community can have in promoting radicalization and extremism.
Realise that we have a duty to keep pupils safe online.

Children are regularly taught about how to stay safe when using the internet and are encouraged to recognise that people are not always who they say they are online. They are taught to seek adult help if they are upset or concerned about anything they read or see on the internet. There are clear rules for using computers in school and an acceptable use agreement for pupils and staff.

At Holly Park we participate in both Anti Bullying week (with a focus on online bullying) and Internet safety Day. Through our curriculum we promote Internet safety and we also buy in an online safety company to run sessions with the children.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **School technical systems will be managed in ways that ensure that the meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **The headteacher / LA officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.**
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place* (to be described) *for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the London USO system

- 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
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords
- 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
- 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.
- 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;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- 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);
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

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, LGfL USO admin site

E-mail

This school

- Provides staff with an email account for their professional use, *London Staffmail / LA email* 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 except for those of the SMT.
- 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. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and school office e-mail
- 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

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom.

At Holly Park (In line with our Acceptable use agreement) staff must not bring in their own ipads or laptops for use in school.

Mobile phones brought into school are entirely at the staff member, student's & 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.

Student mobile phones which are brought into school must be turned off (not placed on silent) and handed in to the school office to be locked away until the end of the school day when they can be collected.

Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras which have been provided by the school.
Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc.

The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only. Staff should not share their personal mobile phone numbers with parents. Parents who accompany a school trip should be given the main school phone number for contact purposes.

On the school site, staff personal mobile phones will only be used with permission from the Deputy Headteacher or Headteacher in an emergency situation.

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, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.
  - *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
  - *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
  - *Pupils must not take, use, share, publish or distribute images of others without their permission*
  - *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
  - *Pupils' full names will not be used anywhere on a website, particularly in association with photographs.*

- 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
- Permission from parents or carers will be obtained before photographs and videos of students / pupils are published on the school website
- Permission from parents or carers will be obtained before photographs of students / pupils are published outside the school
- Pupil's work can only be published outside of the school with the permission of the pupil and parents or carers.
- 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
- Photographs will only be stored off site on password protected PCs by the Headteacher and website administrator.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

Technical solutions

- We require staff to log-out of systems when leaving their computer
- We use encrypted flash sticks and EYFS laptops if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets or in a lockable storage area
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of properly
- Paper based sensitive information is shredded on site in small amounts or larger amounts are collected by secure data disposal service>.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission

Mobile phones may be brought to school	x						x	
Use of mobile phones in lesson time or in offices				x	x			
Use of mobile phones in social time	x				x			
Taking photos on cameras	x						x	
Taking photos on mobile phones				x	x			
Use of other mobile devices eg tablets, gaming devices		x						x
Use of personal email addresses in school, or on school network			x		x			
Use of school email for personal emails				x				
Use of messaging apps					x			
Use of social media			x		x			

When using communication technologies the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while student pupils at KS2 will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on

the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
School staff should ensure that:

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

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Use of/ visiting radicalisation websites					x
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps				X	
Use of video broadcasting eg Youtube		X			

Responding to incidents of misuse

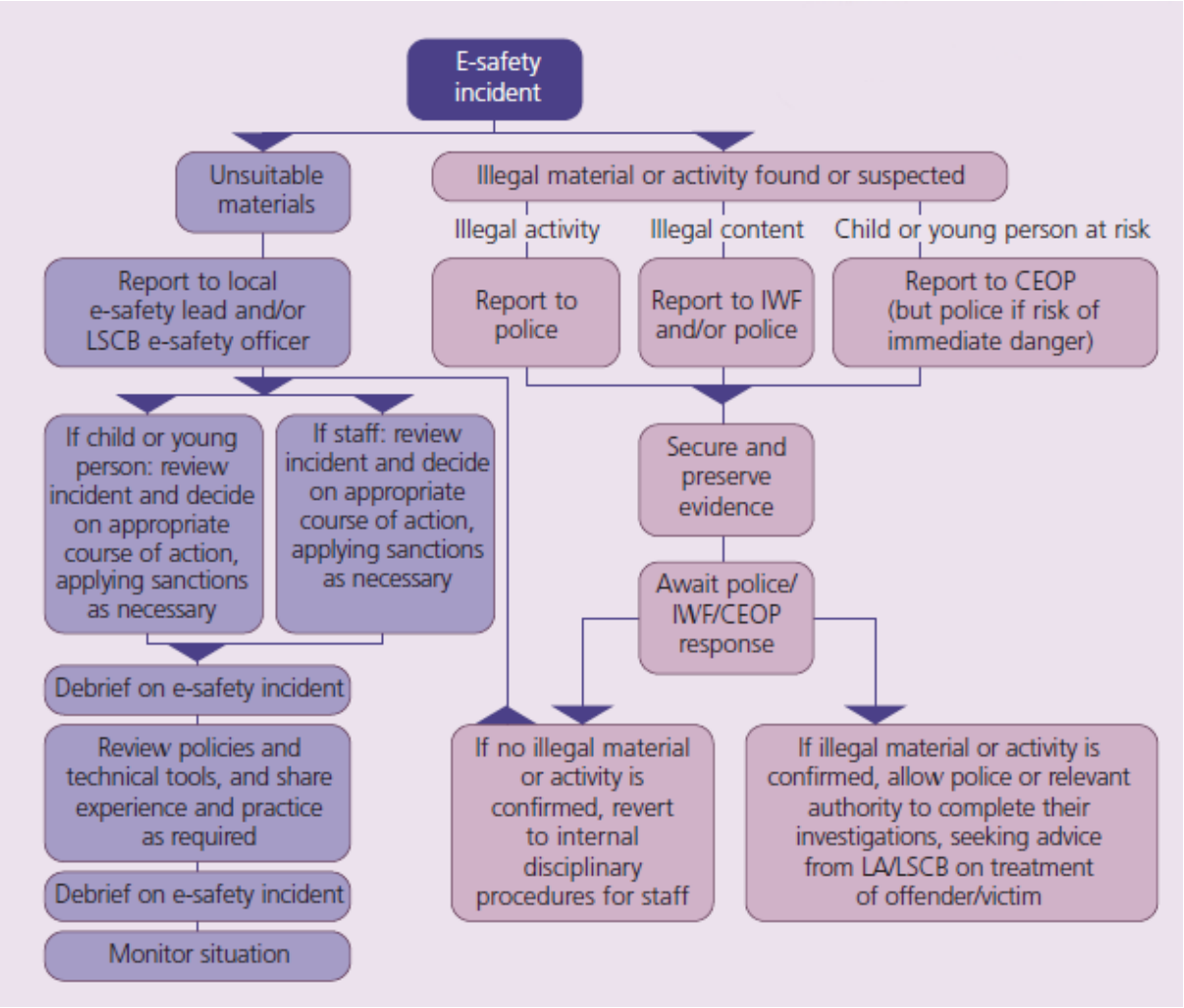
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

4 Key Principles

- Find it
- Report it
- Action it
- Log it

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, radicalisation, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).

- Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

The school will take all reasonable precautions to ensure online-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	

Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Accessing sites that may be linked to radicalisation		x	x	x	x	x		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Accessing sites that are linked to radicalisation or extremism (for themselves or for pupils)		x	x	x	x			x
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X

Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
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.

Schedule for Development / Monitoring / Review

The implementation of this e-safety policy will be monitored by the:	*SMT and Governors*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body* will receive a report on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of*
  - *students / pupils*
  - parents / carers
  - *staff*

Further separate documents:

The Acceptable Use Agreements (AUA) should be signed by staff and retained.

Other related policies:

Safeguarding

Anti-bullying

Data Security

Document Control

Revision History

Version	Revision Date	Revised By	Revision
1.0	November 2014	Ann Pelham	Written as draft version in line with current advice
1.1	March 2015	Ann Pelham	Updated as new Key Leader
1.2	June 2015	Ann Pelham	Updated E-safety training
1.3	October 2015	Govs S&PW	Updated
1.4	March 2016	Ann Pelham	Updated following online -safety & social media training
1.5	September 2016	Govs S&PW	Updated & Reviewed
1.6	September 2017	Govs S&PW	Updated & Reviewed
1.7	Autumn 2018	Govs S&PW	Updated & Reviewed
1.8	Autumn 2019	Govs S&PW	Updated & Reviewed
1.9	Autumn 2020	Govs S&PW	Ratified
2.0	Autumn 2021	Govs S&PW	Ratified

Signed by

	Name	Signature	Date
Headteacher	Ann Pelham		
Chair of Governors	Tim Graveney		

Distribution

Shared with
• Staff via school server • Parents via Website • Staff via Acceptable Use forms signed each academic year • Pupils via computer rules in classroom walls • Pupils via Acceptable Use forms • Governors via committee meetings

Date for next review
Autumn 2022

I will only use polite language when using computers
I must not write anything that might upset someone
I know that my teacher will regularly check what I have done on the school computers
I must not tell anyone my name, where I live or my telephone number over the internet
I must not tell any usernames or passwords to anyone except my parents
I must log off after I have finished with my computer
I must not use the computers in any way that stops other people using them
I will report any websites that make me feel uncomfortable to the teacher
I will tell my teacher if I receive any messages that make me feel uncomfortable
I will not try to harm any equipment or the work of another person on a computer
If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils

Appendix 1

COMPUTER RULES

Pupil Acceptable Use Policy

I agree to follow the school rules when using the school computers. I will use computers sensibly and follow the rules explained by my teacher

I agree to report anyone not using computers sensibly to my teacher

I also agree to tell my teacher if I see websites that make me feel unhappy or uncomfortable

If I do not follow the rules, I understand that this may mean I might not be able to use the computers

Appendix 2

HOLLY PARK
PRIMARY SCHOOL

Data Security Policy
Acceptable Use Staff Agreement Form

This agreement covers the use of digital technologies in school : i.e email, intranet and network resources, learning platform, software, equipment and systems

- I will use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body
- I will not reveal my passwords to anyone to anyone except restricted authorised staff.
- I will not allow unauthorized individuals to access email, internet, intranet, network, or other school/LA systems.
- I will ensure that all sensitive or confidential documents and data are saved, accessed and deleted in accordance with the school's data security and confidentiality protocols. All such data should be held on an encrypted memory stick provided by the school. Reception laptops are encrypted for the EYFS profiles to held on them

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use approved, secure email systems for school business
- I will only use the approved school e-mail or MLE for communication with parents if necessary – e.g PTA business, trips, governors etc
- I will password protect any ipads or iphones that I access my school e-mail from
- 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 leadership team
- I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed
- I will not connect a computer, laptop or other device (including USB flashdrive) to the network/internet that does not have an up to date anti virus software
    - External media must not be used in school unless verified as safe by the ICT team.
    - Anti-virus and firewall must not be disabled.
    - Encryption must not be bypassed.

- I will not bring in from home any other laptop to use other than that given to me by the school
- I will not allow children access to my school laptop
- I will not use camera phones for taking images of pupils. I will only store images of pupils or staff at home with permission of the school.
- I will ensure that my mobile phone is stored away during lesson time in the classroom
- I will use the school's learning platform in accordance with school and London grid for learning advice
- I will ensure that any private social networking sites/blogs that I create or actively contribute to are not confused with my professional role. I will ensure that my security settings are set to high.
- I will not run personal chat/network programs in the background whilst in school.
- I will ensure that any confidential data that I wish to transport electronically from one place to another is protected by encryption and that I follow school data security protocols when using such data in any location
- I understand that data protection policy requires that 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 and network usage can be logged and this information could be made available to the leadership team or governors on request
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

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 agree to abide by all the points above.

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)

Authorised Signature (Head Teacher / Deputy)

I approve this user.

Signature .... Date

Full Name ..... (printed)

Appendix 2

HOLLY PARK
PRIMARY SCHOOL

HOLLY PARK
Pupil Acceptable Use Policy
Online – Health Agreement

All pupils must follow the rules in this policy when using school computers.

Pupils that do not follow these rules may find:

- **They are not allowed to use the computers**
- **They can only use computers if they are more closely watched**

Staff will show pupils how to use the computers.

	Computer Rules
1	I will only use polite language when using computers
2	I must not write anything that might upset someone
3	I know that my teacher will regularly check what I have done on the school computers
4	I must not tell anyone my name, where I live or my telephone number over the internet
5	I must not tell any usernames or passwords to anyone except my parents
6	I must log off after I have finished with my computer
7	I must not use the computers in any way that stops other people using them
8	I will report any websites that make me feel uncomfortable to the teacher
9	I will tell my teacher if I receive any messages that make me feel uncomfortable

10	I will not try to harm any equipment or the work of another person on a computer
11	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils

---

Please return this slip

Pupil Acceptable Use Policy

I agree to follow the school rules when using the school computers. I will use computers sensibly and follow the rules explained by my teacher

I agree to report anyone not using computers sensibly to my teacher

I also agree to tell my teacher if I see websites that make me feel unhappy or uncomfortable

If I do not follow the rules, I understand that this may mean I might not be able to use the computers

Pupil Name _____

Parent/Carer Name _____**Parent/Carer Signature** _____

Appendix 4

HOLLY PARK
PRIMARY SCHOOL

HOLLY PARK PRIMARY SCHOOL

Permission Form

Name of Child _____

Local Walks
I give permission for my child to be taken on short walks around Friern Barnet during his/her time at Holly Park School. I understand that separate letters will be sent out for educational visits that involve a whole day, or those involving the use of public transport or coach hire.
*Please delete as appropriate ***YES / NO**

Reading Books
I would like my child to bring home his/her reading books and library books and agree to pay for any books that are lost or damaged ***YES / NO**

Photographs
I give permission for my child to have their photograph taken whilst participating in school activities and for these to be used in the school's own materials (for example displays, website and prospectus) ***YES / NO**

I give permission for my child to video, and be videoed, as part of curriculum work for use internally by the school ***YES / NO**

I give permission for my child's photograph to be used by other agencies approved by the school (for example the local authority and local press) ***YES / NO**

Plasters
I give permission for a first aider to use plasters on my child ***YES / NO**

Earrings
My child wears earrings and I agree that they will be removed for PE lessons ***YES / NO / N/A**

Head Lice
In the event of an outbreak of headlice in school, I give permission for my child's head to be examined and understand that if lice are found my child will be sent home, where it is my responsibility to treat them before they return to school ***YES / NO**

Dinner Money
I agree that if my child has school dinners I shall pay in full, in advance ***YES / NO**

Computer
I give permission for my child to use the internet under supervision at school in line with the school Internet policy ***YES / NO**
I give permission for my child to use electronic mail under supervision at school in line with the school Internet policy ***YES / NO**

Signed _____ **Date** _____

Name _____

Relationship to child _____

Appendix 5

Google Meet Guidelines

1. Pupil conduct and expectations

- The school will ensure that pupils are aware of the Acceptable Use Agreement – Pupils. This is contained in the admission pack which parents sign as they join the school.
- Pupils will be reminded that they should take part in live online lessons in an appropriate setting, e.g. a quiet space with a neutral background. Any devices should be used in communal areas of your home e.g. in your lounge or kitchen, **but not in bedrooms.**
- Pupils should attend sessions each week and be on time
- Pupils should have their cameras on at all times
- Pupils must wear suitable clothing.
- Pupils will be reminded not to record live online lessons on their devices. Screenshots or sharing of any footage is strictly forbidden.
- Pupils will be reminded not to speak during live online lessons unless they are prompted to do so or have a question about the lesson.
- Pupils will be reminded to adhere to the school's Behaviour Policy at all times during live online sessions, as they would during a normal school day.
- The school will ensure that any pupils who breach the code of conduct will be removed from online sessions and parents contacted.
- Pupils must keep their microphones muted during live video meet ups, until invited to unmute and speak by their teacher.

- A chat function will not be in use and the children should not attempt to write anything in chat.
- Any unacceptable behaviour during a live video meet up will be dealt with in accordance with the school's Behaviour Policy. Unacceptable behaviour may result in a child being asked to leave a meet up immediately.
- Pupils must leave the live video meet up immediately on being instructed to do so by their teacher at the end of the session.

Parent/ Carer Expectations:

- Parents will be provided with a copy of the school Blended Learning Policy and the Live Online Session Home school Policy
- Parents will make sure their child attends the session and is punctual for all live sessions
- Parents/ carers must stay in the room with their child for the duration of the session but should NOT be seen on the screen by other children.
- Parents/ carers must ensure that their child wears suitable clothing, as should anyone else in the household who may pass by the screen.
- Language used by anybody in the household must be appropriate, including any family members in the background.
- Parents/careers will not use Google Classroom to contact a member of staff and will instead use the school office email address.
- Parents/ carers should refrain from interacting with the session. If you have any questions of queries about online sessions or online learning in general, please contact the school office by phone or by emailing office@hollypark.barnet.sch.uk
- Parents/carers should contact the school's Designated Safeguarding Lead (Maria Michael) if they have any safeguarding concerns.

Staff conduct and expectations:

- Staff will be aware of the requirements set out in the Staff Code of Conduct and will ensure they understand their responsibilities with regard to conduct during live online lessons. All teachers will act in accordance with the expectations set out in the school's Staff Handbook and the Staff Code Of Conduct document.

- The school will ensure that staff read, sign and return the Technology Acceptable Use Agreement – Staff annually.

- Staff will only use school-provided email addresses, phone numbers or accounts to communicate with pupils when conducting live online sessions.

- Staff will use school-owned devices for conducting live online sessions, where possible.

- Staff will not share personal information whilst conducting live online lessons.

- Staff will ensure they conduct their live online session from an appropriate location – either the classroom, or if this is not possible, from a quiet area in their home which has a neutral background. For example in a school classroom or in a lounge/ kitchen at home, **but not in bedrooms.**

- Staff will communicate with pupils within school hours

- Staff will only communicate and conduct live online sessions through channels approved by the school.

- Staff will keep a log of anything untoward that happens during live online lessons and report it. E.g. pupil behavioural issues, any incident in their own home that pupils may witness, technical glitches, inappropriate language, parental interference or bad language etc and

ensure it is properly documented in line with the school's Records Management Policy and reported to either the Deputy Head or Computing lead as appropriate depending on the nature of the problem.

- Live sessions should be kept to a reasonable length of time – 30 mins.

- Teachers will group their class into 3 groups of 10 children for meet ups as a minimum. Teachers may prefer to have 4 groups. Please note that children cannot move between groups.

- Teachers will create a weekly timetable for the meet ups and this will be communicated to parents/ carers via the school office and our school messaging service. The time will stay fixed.

- Teachers will keep an attendance register of pupils so we can follow up on pupils who do not attend

- Teachers will enter the live video meet up at the designated start time, and only if they are certain there is more than one pupil present. **Teachers should never be alone with a child in a live video meet up.**

- Teachers will set the behaviour expectations for the children at the beginning of the meet up. They will mute all children's microphones and only unmute children when they are invited to speak.

- Teachers will deal with any unacceptable behaviour in accordance with the school's Behaviour Policy. If a child is behaving inappropriately, the teacher may need to ask the child to leave a session immediately.

- If a teacher feels that a child/ parent or carer is not following the Live Video Safeguarding Expectations, they will ask the child to leave the meet up immediately.

- Language must be professional and appropriate at all times.

- Teachers will ask all pupils to leave the live meet up at the end of the session and then end the meeting.

- Members of the school's Senior Leadership Team may attend a selection of meet ups and monitor class areas on Google Classroom to ensure that the Safeguarding Expectations are being adhered to by children, parents and staff.