HIGHSHORE SCHOOL

ONLINE SAFETY POLICY

APPROVED BY GOVERNORS ON

DUE FOR REVIEW -
RESPONSIBLE PERSON – HEADTEACHER

SIGNED BY

CHAIR OF GOVERNORS S Smith

HEADTEACHER

www.esafety.lgfl.net

Policy: The Acceptable Use of the Internet and related Technologies

Contents

Page

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. 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
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio/ video broadcasts downloaded to computer, MP3/4 player, mobile device such as a tablet or smart phone)
- Social networking sites
- Video broadcasting site Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones/ tablets with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT 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 online safety education programme for pupils, staff and parents.

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 the online safety co-ordination.

Our school **online safety Co-ordinator** is Mike Barrett.

Our online 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 The Child Exploitation and Online Protection (CEOP)[1]. The school's online safety coordinator ensures the Head, senior management, DSL's and Governors are updated as necessary.

Governors need to have an overview understanding of online safety issues and strategies at this school.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These procedures now extend to monitoring acceptable and safe use of online, live video platforms such as Zoom (the school's preferred form of this type of platform). The school, through the Computing/ ICT lead teacher and online safety co-ordinator has produced guidelines for teachers and families on safe use of online/remote learning platforms (see appendix 1). 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, digital cameras, tablets and live video remote learning/ meeting platforms such as Zoom and Microsoft Teams.
- publication of pupil information/photographs and use of website;
- e-bullying / Cyberbullying procedures across all media platforms.
- their role in providing online safety education for pupils in school, off-site and across remote learning platforms.

Staff are reminded / updated about online safety matters at least once a year through new staff induction training and teacher/ support staff meetings

The school includes online safety in the curriculum and aims to ensure that every pupil has received guidance about safe and responsible use appropriate to their needs and level of usage. Pupils need to know how to control and minimise online risks and how to report a problem.

The school ensures that they make efforts to engage with parents over online safety through parent training, regular updates through letters/ school website and that parents/guardians/carers have signed and returned an online safety/AUP form.

4. Communications

Pupils

Pupils' perceptions of the risks may not be mature; the online safety rules may need to be explained or discussed.

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

Useful online safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com
- Online safety will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

Staff

Staff should feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. These strategies will include engaging pupils in remote, online learning where appropriate aiming to be fully inclusive.

Staff must understand that the rules for information systems misuse. 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 and online safeguarding scenarios used in safeguarding induction training.

- Staff training in safe and responsible Internet use and on the school online safety Policy will be provided as required.

Parents

Internet use in pupils' homes is increasing. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. Through a partnership approach the school may be able to help parents plan appropriate supervised use of the Internet at home. The school aims to provide update information sharing on internet safety matters through the school website, newsletter and guidelines for safer internet use.

5. How will complaints regarding online safety be handled?

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, mobile device or remote online platforms. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

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

- interview/counselling by teacher/online safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period

Our online safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Policy - Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; ICT is a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently, safely and to develop a responsible and mature

approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide; • collaboration between pupils, professionals and across sectors;
- Access to learning wherever and whenever convenient including off-site remote interactive lessons through online meeting platforms (Zoom)

The Internet enhances the school's management information and business administration systems through, for example:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- Secure data exchange between local and government bodies.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

Technology at Highshore School:

- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Has additional user-level filtering in-place using the LGfL USO service.
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Closely supervises any pupil accessing the Internet;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;

Education and training:

Pupils (and staff) need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or ICT manager for inclusion in the list of blocked sites.

Pupils and staff must learn to recognise and avoid risks online – to become 'Internet Wise'. To STOP and THINK before they CLICK. Both need to understand how to ensure personal information is, and remains, private.

Staff must not confuse or compromise their professional role with any personal online activity, for example inviting pupils into their personal social networking site. Staff must also be aware of remote online learning acceptable use and protocol. If they are unsure or become aware of any inappropriate behaviour during such learning sessions they must report these through the school's safeguarding procedures.

Pupils need to understand the dangers of using unfiltered web access outside school at a location where parental controls or filtering have not been enabled. Pupils should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website, in a message or in a social networking environment..

Pupils and staff need to know how to deal with any Cyber Bullying incidents. Pupils need to know about the national agencies, such as Child Exploitation Online Protection (CEOP), http://www.ceop.gov.uk/ – so that in an extreme case, they know how to "report abuse".

Highsore 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;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and tell a member of staff.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- 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 know some search engines / web sites that are more likely to bring effective results;
    - 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, 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;
    - how to behave appropriately during remote online learning sessions

Policy: managing e-mail

E-mail is an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed use of regulated e-mail in schools can bring significant educational benefits, increasing the ease of communication within the school community and facilitating local and international school projects.

However, e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Use of freely available, unregulated email within a school is not appropriate.

Technology:

Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. Schools in London have appropriate educational, filtered Internet-based e-mail options through the London Grid for Learning (LGfL).

LondonMail is an email solution, which is filtered for inappropriate language and unsolicited mail, designed for pupil use. It uses a common format for identity but at the same time appears anonymous. This means a pupil's school (and thus their age group, gender and location) are not identifiable.

e.g. jbloggs031.301@lgflmail.net

Although this seems anonymous, because the account is linked to an LGfL sign-on database (USO) the account is always accountable and traceable.

StaffMail is available to staff and governors within LGfL connected schools and LAs. It has the full functionality of a Microsoft Exchange account. It is only accessible where the LA has Unified Sign On (USO) in place. The service is suitable for those LAs that do not have a LA Corporate email system.

Procedures:

In the school context, e-mail should not be considered and Highshore School reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail, will not be used in schools and staff are required to use appropriate LA or LGfL systems for professional purposes.

Many teenagers will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. These should not be used for school purposes. Where e-mail accounts are not monitored, there is the risk that pupils could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring and tracing very difficult and require support from the providers of the email system (who may be an international company).

Email must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured email system.

Education:

Staff and pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's online safety and anti-bullying education delivered by the PSHE curriculum.

Policy – Use of digital and video images

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff oversees /authorises the website's content and check suitability.

Use of still and moving images

Care is taken when using photographs or video footage of pupils on the school website. The first and last name will not be used with a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

If the pupil is named, avoid using their photograph / video footage.

If the photograph /video is used, avoid naming the pupil.

If the school website is using a webcam – then this will be checked and monitored to ensure misuse does not occur accidentally or otherwise.

The school has adopted the trial use of an online communication/ sharing platform, Class Dojo. This allows teachers to communicate with parents directly and to share class success digitally. All parties involved, families and teachers must sign an agreement form which adheres to the safeguarding procedures set out in the Class Dojo terms and conditions of use (see appendix 2 – Class Dojo.com/terms and conditions). Photos can be shared in real time of pupil work success with individual parents and direct teacher contact parents only have access to their own child's account area.

Technical:

Digital images / video of pupils will be stored securely on the school network and old images deleted after a reasonable period.

Education:

Staff should report any inappropriate use of images to a member of the senior leadership team and understand the importance of safe practice. Pupils should be encouraged to report such images to staff. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

At Highshore School

- The Headteacher and the communications manager take overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the and the communications manager and other specific members of staff.
- 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 and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- 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;
- Digital images /video of pupils are stored in the multimedia folder on the network and images are archived at the end of the year in a secure storage area on the school system.
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

Policy – Managing equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students 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 Highshore School:

- Will ensure staff read and sign that they have understood the school's online safety Policy.
- Provides pupils as appropriate with an individual e-mail log on;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Has set-up the network so that users cannot download executable files / programmes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed including PAT testing and cleaning of projector filters.
- 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;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school systems:
- 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 for technical support for IT technical support; network system diary support.
- Uses the DfES Secure Access Arrangements for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.
- Teaching staff will be able to log into the school system remotely via a secure platform to mitigate the need for transfer of data via a USB memory stick or other storage device.
- Remote, online learning records are kept by teachers and regularly checked by SLT.

Policy – How will Infringements be handled

Whenever a student or staff member infringes the online safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as examples only:

Students

Category A infringements

- Use of inappropriate internet sites
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in school
- Use of unauthorised instant messaging / social networking sites

If the infringement has been knowingly committed the matter will be investigated by the class teacher

Category B infringements

Where a pupil or young person knowingly

- Continues use of inappropriate sites after being warned
- Continues unauthorised use of email after being warned
- Continues unauthorised use of mobile phone (or other new technologies) after being warned
- Continues use of unauthorised instant messaging / chatrooms, social networking sites, News Groups
- Corrupts or destroys others' data without notifying a member of staff.
- Accesses offensive material and does not log off or notify a member of staff of it

Such incidents would be referred to the SLT and internet access/ mobile device will be removed for an appropriate period.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Such incidents would be referred to the Online safety co-ordinator, Deputy Head teacher or Head Teacher and parents may be contacted.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / LGfL as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Such incident would be referred to the Head teacher and Parents would be contacted. The Community Police Officer may be involved.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. On-line shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff members professional standing in the school and community including inappropriate use of social networking sites
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Sanction - **referred to line manager / Headteacher**. Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Sanction – **Referred to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police

Other safeguarding actions:

Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team. This may also be with the assistance of the GDPR support organisation, Judicium.

Child sexual abuse images found?

In the case of child sexual abuse images being found, the member of staff should be **immediately suspended** and the Police should be contacted: free phone: **0808 100 00 40**

You should also report to your Local Authority LSCB Designated Officer.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's online safety / Acceptable Use Policy. All staff will be required to sign the school's online safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Where appropriate Pupils will sign an age appropriate online safety / acceptable use form;
- The school's online safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on online safety issues.

Online safety agreement form: parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, London Grid for Learning (LGfL) e-mail and other ICT facilities at school.

I know that where appropriate my daughter or son has signed an online safety agreement form and been shown the 12 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their online safety or e-behaviour that they will contact me.

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 online safety.

Parent / guardian signature: _____

Date: ___/___/___

Use of digital images - photography and video: **I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.**

Parent / guardian signature: _____ Date: ___/___/___

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

In the event of school closure due extenuating circumstances such the Coronavirus pandemic the school may move performances such as Christmas shows to an online platform (Zoom) where parents will be invited to book e-tickets and by doing so agree to safeguarding rules set by the school. The school will also follow the checklist set out in appendix 3.

Only images of pupils in suitable dress are used.

When working remotely from home pupils, families and staff are expected to follow appropriateness of dress as per guidelines in appendix 1.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

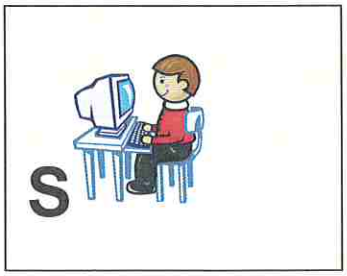
- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's photo could appear in the media if a newspaper photographer or television film crew attend an event.
  - Your child's image be used in a remote online learning lesson to demonstrate good practice to other learners as part of that lesson.
  - Remote learning lessons will never be recorded as per appendix 1 guidelines.
  - If your child's class uses Class Dojo photos and work will be shared with you through the individual account created via this digital platform. This may only be done with your consent through signing the terms of agreement and consent form sent to you when Class Dojo is ready for your child and family use.

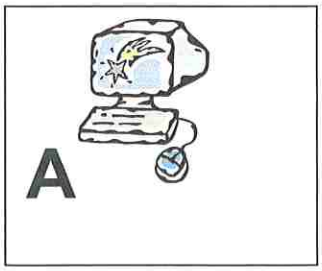
Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

E - safety form for pupils

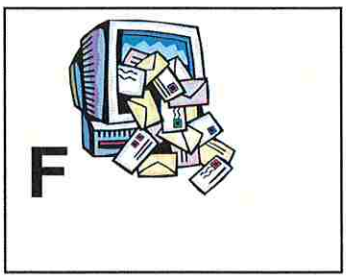
Think before you click



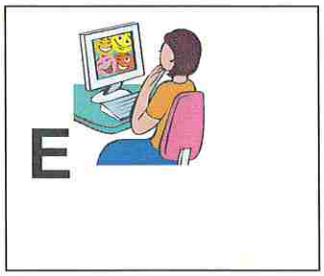
I will only use the Internet and email with an adult



I will only click on icons and links when I know they are safe.



I will only send friendly and polite messages



If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only 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 any personal password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / 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 not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business which is currently staffmail unless approved by the Head Teacher.
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate 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 line manager / e safety 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 connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- If applicable, I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice this includes the preferred remote online learning platform (Zoom)
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and will not in any way bring the school or colleagues into disrepute by inappropriate postings on social networking sites.
- 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 ensure that any equipment taken out of school on loan other than during school visits will be my responsibility and should loss/damage occur liability will be covered by personal insurances.
- 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 will use the school's secure log on in the first instance when working off-site.
- 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 online safety curriculum into my teaching/ working practises.
- I will only use LA systems in accordance with any corporate policies.

- I understand that all Internet usage and e-mails can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- When using a sharing platform such as Class Dojo I will only share photos and work where parents have signed appropriate consent forms

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 online 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)

Job title ..... School

.....

Authorised Signature (Deputy Head Teacher/School Business Manager I

approve this user to be set-up.

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

Full Name ..... (printed)

Guidance: Safeguarding and Protecting Children

What are the online safety issues?

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with.
This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.

An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text/ instant chat message platform such as What's app, Snapchat and Instagram and is therefore harder for schools to notice and deal with.

Section 175 of the 2002 Education Act and Section 11 of the 2004 Children Act places upon all those who work with children a duty to safeguard and promote their welfare by creating a safe learning environment and where there are child welfare concerns, taking swift action to address them. It is vital that schools are aware of the signs which might indicate that a child is being groomed, bullied or being subjected to inappropriate material and know how to take steps to begin to address this and safeguard and support the child.

Creating a safe learning environment means having effective arrangements in place to address a range of issues and schools should ensure that they have policies and procedures in place which are reviewed annually and adhered to by all staff, teaching and non-teaching whether in a paid or voluntary capacity.

Guidance: Cyberbullying

Key national document :
"Cyberbullying – Safe to Learn: Embedding Antibullying work in schools" DCSF-00658-2007

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (eg: What's app) or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e.mail (such as 'Happy Slapping' videos)

It should be noted that the use of ICT to bully could be against the law.
Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984* for example.

Bullying is when someone deliberately hurts you or makes you unhappy. It will be repeated and be difficult to defend yourself against it. Bullying can be racist, sexist or homophobic.

Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the bullied emotionally and/or physically.

The following will be appended to our **Anti-bullying Policy**

Highshore School will not tolerate the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff.

We consider that bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

3. *Advise the child not to respond to the message*
4. *Refer to relevant policies including online safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions*
5. *Secure and preserve any evidence*
6. *Inform the sender's e-mail service provider*
7. *Notify parents of the children involved*
8. *Consider informing the police depending on the severity or repetitious nature of offence*
9. *Inform the online safety co-ordinator.*

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. *Inform and request the comments be removed if the site is administered externally*
2. *Secure and preserve any evidence*
3. *Send all the evidence to online safety co-ordinator.*
4. *Endeavour to trace the origin and inform police as appropriate*

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.
"

Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/ deputy head teacher/ e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered. **An inappropriate website is accessed <u>intentionally</u> by a child.**
   Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
4. Notify the parents of the child.
5. Inform the school technicians and ensure the site is filtered if need be.
6. Inform the LA if the filtering service is provided via Lgfl. **An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   Remove the PC to a secure place.
   Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   Identify the precise details of the material.
   Take appropriate disciplinary action (contact Personnel/Human Resources).
   Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   Contact the local police or High Tech Crime Unit and follow their advice.
   If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

10. Advise the child not to respond to the message.
11. Refer to relevant policies including online safety anti-bullying and PHSE and apply appropriate sanctions.
12. Secure and preserve any evidence.
13. Inform the sender's e-mail service provider.
14. Notify parents of the children involved.
15. Consider delivering a parent workshop for the school community.
16. Inform the police if necessary.
17. Inform the LA online safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Endeavour to trace the origin and inform police as appropriate.
4. Inform online safety co-ordinator.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Consider the involvement police and social services.
4. Inform LA safeguarding officer.

All of the above incidences must be reported immediately to the head teacher and online safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet/ mobile technology: they must be able to do this without fear.

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.

- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.
- I will adhere to the remote online learning guidelines set out in appendix 1.

Appendix 1

Highshore Guidelines for Staff delivering Remote Learning

1. Explicit and informed parental consent has been secured for their children to participate in livestreamed lessons
2. The platform and methodology being used to provide livestreaming has been risk assessed in the context of the school's policies on:
    - •safeguarding;
    - •data protection; and
    - •health and safety
3. Safeguarding protocols continue to be followed at all times
4. Livestreaming will take place during what would be normal pupil session times when the school premises are fully open
5. Livestreaming will be undertaken through the use of an employer-approved rather than personal account
6. The technology they use allows them to blank out or distort their backgrounds
7. Sessions including students are not to be recorded
8. Keep a log of taught sessions and who was present appendix 1a
9. Live lessons will not be recorded

Remote Learning Agreement
for parents and guardians

1. Find a safe and relatively private place to conduct the session
2. Ensure that everyone involved is dressed appropriately
3. Try to ensure that only the agreed people are on screen
4. Please encourage your child and all present to use appropriate language and behaviour

5. Please try to have any learning resources (e.g. worksheets, pens) needed for the session ready beforehand
6. If you require any resources please contact the school for assistance
7. If you require technical assistance please inform the school
8. Please do not record the session
9. Please try to join the session at the agreed time
10. If you are unable to attend, please let the teacher know

Appendix 1a

Remote Learning Log

Date:			
Teacher:			
Name of pupil	**Description of learning activity**	**Approximate time to complete (minutes)**	**Other comments**

Appendix 2

ClassDojo.com\terms and condition

Example letter for CLASSDOJO

Dear Parents/Carers,
In order to improve and enhance Home/School communications, (Class name) have been chosen to trial a programme called **'ClassDojo'**.
ClassDojo is a school communication platform that teachers, students and families can use every day to build close-knit communities by sharing what's being learned in the classroom through photos, videos and messages. The students currently use it as a form of feedback during the school day.

A part of this platform is photos and videos, which are uploaded onto the website. Only the teachers and parents of (Class name) will have access to this media. The aim of uploading this media is to regularly share with you what your children are learning and how they are progressing in school each day. Please fill in the consent form below to advise us whether you give permission for photos and videos to be used on ClassDojo.

We are asking that parents register themselves with ClassDojo so that we can trial it over the next half term. Attached to this letter is the instructions needed to log in and view your child's progress.

If there are any queries about ClassDojo, please do not hesitate to contact myself.

Yours Sincerely,

Class Teacher

MEDIA CONSENT

Child name: _____

Please circle your answer

1. May we use your child's photograph in images on ClassDojo? Yes/ No
2. May we use your child's videos on ClassDojo? Yes/ No
3. May we share your child's work on ClassDojo? Yes/ No

Signed: _____ Date: _____

Appendix 3

Highshore Online performance checklist

Have parents/children given consent?	The performance is not being recorded so not shared outside of the school community. Sharing of play is 'live' so school play usual procedures apply
Have acceptable use agreements been signed by staff, pupils and parents?	What are these? Staff/ pupils and families have signed acceptable use policies in general in terms for using school IT/ mobile devices.
Have appropriate risk assessments been carried out?	Create RA
How long will the performance be available/ retained for?	Performance only retained on school secure server so no sharing implications
What technology will be used?	Zoom

Is there tech support available?	Nick
What's the minimum age requirement for the chosen platform?	n/a
Are the devices being used secure?	Yes – LGFL and all safeguarding procedures on Zoom are in place
Have the chosen platform's privacy policies been reviewed by the school?	Yes - https://blog.zoom.us/zoom-privacy-policy/ https://zoom.us/privacy?_ga=2.64907183.1282006670.1606823553-2134634398.1604406371 Specific Privacy policy based on school's n/a as it is for remote learning and student login etc
Do audience members understand the ground rules?	Create guidelines Info to be shared with invite and newsletter
Have notifications outlining expected etiquette been given to pupils, staff parents and carers?	Create guidelines Info to be shared with invite and newsletter Zoom guidelines created for parents/ families, staff

Next Steps

Confirm Acceptable use signed?
Create performance risk assessment?
Create registration for performance
Create guidelines to be shared with invite details and newsletter