ONLINE SAFETY POLICY

WORMHOLT PARK PRIMARY SCHOOL

Article
Every child has the right to privacy

REVIEWED:	AUTUMN 2020
NEXT REVIEW DATE:	AUTUMN 2023

Contents

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Wormholt Park School with respect to the use of IT-based technologies.
- Safeguard and protect both the children and staff of Wormholt 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, and personal use.
- Have clear structures to deal with online abuses 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.

This policy is written in line with 'Keeping Children Safe in Education' 2018 (KCSIE) and other statutory documents; it is designed to sit alongside Wormholt Park's statutory Safeguarding Policy. **Any issues and concerns with online safety must follow the safeguarding and child protection procedures.**

The main areas of risk at Wormholt Park School can be summarised as follows:

Content

- Exposure to inappropriate content; whether through age inappropriate sites, hate sites, self-harm sites etc.

Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming
- Online bullying in all forms
- Identity theft and stealing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Age inappropriate behaviour eg: sexting
- Copyright issues

Scope of Policy

This policy applies to all members of the Wormholt Park School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school computers and systems, both in and out of school.

For the specific guidance we give to pupils, see our pupil Acceptable Use Policies

The Education and Inspections Act 2006 empowers Head Teachers to such an 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 online bullying, or other online safety incidents covered by this policy, which may take place outside of the school building, 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 template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Wormholt Park School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and responsibilities

This school is a Rights Respecting community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

All quotations used to outline roles below, unless stated otherwise, are from *Keeping Children Safe in Education 2018*.

Role	Key Responsibilities
Head Teacher	● To take overall responsibility for online safety provision ● To take overall responsibility for data and data security (SIRO) ● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL ● To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant ● To be aware of procedures to be followed in the event of a serious internet safety incident ● Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the governors and other stakeholders to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

Designated Safeguarding Lead	● "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." ● Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." ● "Liaise with the local authority and work with other agencies in line with Working together to safeguard children" ● Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying ● To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents. ● Facilitate internet safety training and advice for all staff, with support from the Computing Subject Lead ● To be involved in the reviewing and updating of this policy and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
All staff	● Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up ● Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures. ● To read, understand and help promote the school's internet safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy ● To have Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections) ● To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor

	their use and implement current school policies with regard to these devices ● Notify the Computing Subject Lead if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Computing Lead	● To promote an awareness and commitment to online safeguarding throughout the school community ● To ensure that online safety education is embedded across the curriculum and taught consistently in each term and in all year groups ● To liaise with school Computing technical staff ● To communicate regularly with the Head Teacher/SLT in the event of a serious online safety issue ● To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident ● To ensure that an online safety incident log is kept up to date ● To liaise with the Local Authority and relevant agencies ● Stay up to date with the latest trends and regulation in online safety ● To ensure there is open communication with the Designated Safeguarding Lead concerning online safety issues and that the clear overarching responsibility for online safety is not compromised ● To be involved in the reviewing and updating of this policy and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees. ● To ensure all software and applications installed for pupil use is age-appropriate and safe for pupils to use. -All staff must read KCSIE Part 1 and all those working with children Annex A -It would also be advisable for all staff to be aware of Annex C (online safety)
Governors	● To ensure that the school follows all current online safety advice to keep the children and staff safe ● To approve the online safety policy and review the effectiveness of the policy ● To support the school in any initiatives aimed at encouraging better online safety ● To “Ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of Designated Safeguarding Lead [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate

	status and authority [and] time, funding, training, resources and support…" ● To "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction [and] regularly updated […] in line with advice from the LSCB […] online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach." ● To "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". ● To "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology."
Technician/Support Company	● To report any online safety related issues that arise, to the Computing Lead at school ● To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ● To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) ● To ensure the security of the school IT system ● To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • **To ensure** the school's policy on web filtering is applied and updated on a regular basis • Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc • Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team • To ensure that he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Computing Lead for investigation ● To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. ● To keep up-to-date documentation of the school's online security and technical procedures

Teachers	● To embed online safety issues where relevant in the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including home learning and extended school activities if relevant) ● To ensure that pupils are aware of legal issues relating to electronic content such as copyright laws (as necessary)
RE and PSHE subject leads	The following is to be considered in accordance with the DfE press release on 19 July 2018 on New relationships and health education in schools. The expectations will be in effect from September 2019 for September 2020, according to the London Grid for Learning. ● Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds." ● Work closely with the Designated Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RE / RSE
Pupils	● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the use of mobile phones and other devices. ● Have an awareness of what websites, applications or other media (including social media) is appropriate for their age and legal age restrictions for certain media exist. ● To know and understand school policy on the taking / use of photos, social media groups and on cyber-bullying. ● To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school ● To have an understanding of the need to avoid plagiarism and uphold copyright regulations. ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

Parents/carers	● To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images ● To consult with the school if they have any concerns about their children's use of technology ● To have an awareness of their children's online activity and what activity is appropriate for their children's age.
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any technology based equipment or the Internet within school ● Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be held in personnel files
- Assemblies will reinforce messages contained within the policy

Handling complaints:

- 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.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - Discussion with teacher/SENCO/Head Teacher etc.
    - removal of Internet or computer access for a period
    - referral to LA / Police.

- The Designated Safeguarding Lead acts as first point of contact for any complaint involving internet safety concerns. Any complaint about staff misuse will be referred to the Head Teacher.

- Complaints of online bullying 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.

Review and Monitoring

The online safety policy is referenced from within other school policies: Computing policy, Safeguarding policy, Anti-Bullying policy, Behaviour policy, and Personal, Social and Health Education policies.

- The school has a Computing Lead who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by staff and approved by Governors. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil online safety curriculum

This school

- Teaches online safety awareness and digital literacy in across years 1-6 every term as a minimum.
- Has a clear online safety education programme as part of the Computing and PHSE curriculums. It is built on LA / LGfL online safeguarding principles and online literacy national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To follow the Kidsmart SMART rules of Internet use (which incorporates keeping information private, not meeting strangers who have been met online, only accepting communication from unknown people, understanding that not all information online is reliable and informing trusted adults if something online makes them uncomfortable/worried) in relation to the rights of the UNICEF Convention on the rights of the Child. ***(Articles 15, 19 and 24)***
    - [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 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;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of online bullying, sexting, extremism 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 online bullying beyond a trusted adult eg: an organisation such as ChildLine.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

Staff training

This school

- Ensures relevant staff knows how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

- Makes regular training available to staff on online safety.
- Provides, as part of the induction process, all new staff with information and guidance on the online safety policy and the school's Acceptable Use Policy.

Parent awareness and training

This school

- Runs a programme of advice and guidance for parents / carers, including:
    - Introduction of the ideas within the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear.
    - Information in school newsletters and on the school web site regarding national support sites for parents.
    - Information about age appropriate web-site and support in engaging children to make responsible choices in their online activity.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on online bullying.

Incident Management

In this school:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.

- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
- Parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Social Media

Wormholt Park School's social media presence

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first researching the school online, and the Ofsted pre-inspection check includes monitoring what is being said online.
Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

A core team of staff takes overall responsibility for managing any social media accounts alongside management of the school website. These accounts may be used to respond to general enquiries about the school, but we ask parents/carers not to use these channels to communicate about their children.

Staff, pupils' and parents' social media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in our Acceptable Use Policy, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.
If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils are not allowed to be 'friends' with or make a friend request* to any staff, governors, volunteers and contractors or otherwise communicate via social media. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member). Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

5. Managing the IT and Computing infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;

- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network
- Only unblocks other external social networking sites for specific purposes
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Is vigilant in its supervision of pupils' use at all times
- Ensures all staff have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: e.g. LGfL secure platforms such as J2Bloggy, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Kiddle or Google Safe Search
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing Lead, who logs or escalates as appropriate to a technician or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**

  This school

  - Uses individual, audited log-ins for all users - the London USO system;
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Ensures the Computing Lead is up-to-date with LGfL services and policies
  - Ensures that the storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school*:*

- Ensures staff read and sign that they have understood the school's online safety policy. Following this, they are set-up with Internet, email access and network access. Email access is through a unique, audited username and password. We also provide a different username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have their own class based username which gives them access to the Internet.
- 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 curriculum network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they **DO** switch the computers off at the end of the day so that daily back-ups can take place.
- Has set-up the network so that users cannot download executable files / programmes
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;

- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that the staff is responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by Computing Lead/Site Manager; equipment installed and checked by approved suppliers
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- 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 SIMS Support, our Education Welfare Officers accessing attendance data on specific children
- Makes clear responsibilities for the daily back up of SIMS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level standards suitable for educational use;
- 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 IT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff must always keep their email password private, must not share it with others and must not leave it where others can find it;

We require staff to use unique passwords for access into the SIMS system, the local school network and for Virtual Learning Environments (VLE).

E-mail

This school

- Provides staff with an LGfl email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website and instead uses anonymous or group e-mail addresses, for example info@wormholtpark.lbhf.sch.uk
- Will ensure that email accounts are maintained and up to date
- Will ensure that pupils can only access email through the LondonMail / PupilMail system from LGfL TRUSTnet
- 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 emails 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

- A core team of staff 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
- Photographs published on the web do not have 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;

Social networking

- The school operates a Twitter account, which is managed and maintained by the School Business Manager. The same rules apply as with the school website regarding the publishing of pupils' names and the content is purely school-based updates and will not contain any personal opinions.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- 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 stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
  All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school. All pupil devices are to be kept in the school office if brought to school.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such devices will be set up in accordance with the rest of the school's network so that only those features approved of by the school's filtering features will be available.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their internet safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.