Osidge
School

Online Safety Policy 2020-21

This forms part of the Safeguarding Policy

School Online safetyCo-ordinator	**Chrisanthy Dyer**
School Designated Teacher forsafeguarding	**Sarah Ostroff**
School named Governor forsafeguarding	**Hasip Mahir**

OurOnline Safety Policy has beenwrittenbased ontheLondonGridfor Learning (LGfL) exemplar policy. It will be agreed by the senior management and then will be approved by Governors. Itwillbe reviewedannually.

Online Safety Policy Overview

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for userstoenablethemtocontrol theironlineexperiences.

Ofsted(2009):Agoodschool'integratesissuesaboutsafetyandsafeguardingintothe curriculum so that pupils have a strong understanding of how to keep themselves safe. The school is pro-active in building on collaborative working with other key agencies to reduce the riskof harmto pupils.'

The school's online safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Securit

School Online safety Policy

Our online safety Policy has been written by the school It has been agreed by the senior management team and approved by governors in September 2009.
The online safety Policy will be reviewed annually by the Computing Lead and HeadTeacher. The

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with staff at the start of each year.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Osidge School withrespecttotheuseofICT-basedtechnologies.
- Safeguard and protect the children and staff of Osidge School.
- Assistschoolstaffworkingwithchildrentowork safelyandresponsiblywiththe internet and other communication technologies and to monitor their own standards andpractice.
- clear expectations of behaviour and/or codes of practice relevant to responsible use ofthe internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other schoolpolicies.
- Ensurethatallmembersoftheschoolcommunityareawarethatunlawfulorunsafe behaviour is unacceptable and that ,where appropriate, disciplinary or legal action will be taken.Anymaterialthattheschoolbelievesisillegalmustbereportedtoappropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation & Online Protection Centre).
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:
Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- life style websites ,for example pro-anorexia/self-harm/suicide sites
- hatesites
- content validation: how to check authenticity and accuracy of online content

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupilachievement, to support the professional work of staff and to enhance the school's management informationand administrationsystems.Internetuseispartofthestatutorycurriculumandanecessary tool for learning. It is an essential element in 21st century life for education, business and socialinteraction.AccesstotheInternetis thereforeanentitlementforpupilswhoshowa responsibleand mature approachto its use.Our school has aduty to providepupils withquality InternetaccessPupilswillusetheInternetoutsideschoolandwillneedtolearnhowtoevaluate Internet informationand to takecareof their ownsafetyand security.

Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, communityusers)whohave access toandareusers ofschoolICTsystems,both I nandoutoftheschool.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulatethebehaviourofpupilswhentheyareoffthe*school*siteandempowersmembersofstaffto impose disciplinarypenaltiesfor inappropriatebehaviour.This is pertinenttoincidentsof cyber-bullying, or other online safety incidents covered by this policy, which may take place outside ofthe school,butislinkedto membershipoftheschool. The2011EducationActincreasedthese powers with regard to the searching for and of electronic devices and the deletion of data (see appendixfor policy).Inthecaseof bothacts, actioncanonly be takenoverissues coveredby the publishedBehaviourPolicy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies andwill,whereknown,informparents/carersofincidentsofinappropriate online safety behaviourthat takeplaceoutof school

The Technologies

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

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple webcams
- Blogs(an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.facebook.com , www.myspace.com / www.piczo.com / www.bebo.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and videofunctionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

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 Head Teacher ensures that the Policy is implemented and compliance with the Policymonitored.
The responsibility for online safety has been designated to a member of the school improvement team alongside our designated teacher for safeguarding.

Our online safety officer is Chrisanthy Dyer

Our **Designated Safeguarding Lead is** Sarah Ostroff. Our Deputy CPOs are JenBrodkin, Chrisanthy Dyer, Siobhan Norman

Our **Safeguarding Governor** is Hasip Mahir.

Ouronline safetyCoordinatorensures theykeepup todatewithonline safetyissues and guidance Through liaison with the Local Authority online safety Officer and through organisations such as Becta and The Child Exploitation and OnlineProtection(CEOP)1. The school's online safety coordinator ensures the Head, senior management and Governors are updated as necessary.
The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors:

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

Governorsareresponsibleforthe approvalof the Online safety Policyand for reviewing the effectivenessofthe policy.Thiswill be carriedoutbythe Governors receivingregularinformation about online safety incidents and monitoring reports. A member of the Governing Body hastakenontheroleofSafeguardingGovernor.TheroleoftheSafeguardingGovernor will include:

- regular monitoring of online safety incident logs
- reporting to relevant Governors/committee/meeting

Head Teacher and Senior Leaders:

The *Head Teacher* has a duty of care for ensuring the safety (including online safety)of members of the school community. The Head Teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Head Teacher and Senior Leaders are responsible for ensuring that the Online safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety role sand to train other colleagues, as relevant.
  The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also to offer support to those colleagues who take on important monitoring roles.

Online safety Coordinator:

- leads on online safety
- takes day today responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of anonline safetyincidenttakingplace.

- provides training and advice for staff
- liaises with the Local Authority/ relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future e-safety developments,
- reports to *governors* to discuss current issues, review incident logs and filtering / changecontrol logs
- attends relevant meeting / committee *of Governors*
- reports regularly to Senior Leadership

ICT Technician:

The ICT technician is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required online safety technical requirements and any *Local Authority / other relevant body* Online safety Policy / Guidance that mayapply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is notthesole responsibilityof any singleperson
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access /email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher / Principal / Senior Leader; Online safety Coordinator

Teaching and Support Staff

All staff are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current *school* online safety policy and practices including Safe use of e- mail; Safe use of Internet including use of internet-based communication services, such as instant messaging and social network; Safe use of schoolnetwork, equipment and data; Safe use of digital images and digital technologies, such as mobile phones and digital cameras; publication of pupil information/photographs and use of website; eBullying / Cyberbullying procedures**
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the *Head Teacher* for investigation /action/ sanction
- online safety issues are embedded all aspects of the curriculum and other activities
- students / pupils understand and follow the online safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyrightregulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessonsand other school activities (where allowed) and implement current policies with regard to thesedevices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safetyprocedures.

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

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

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

Staff are reminded / updated about online safety matters at least once a year. We have a whole school focus on onlinesafetyannuallyon onlinesafetyday in February.

Child Protection / Safeguarding Designated Person

They should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the *school* digital technology systems in accordancewith the Pupil Acceptable UsePolicy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyrightregulations
- need to understand the importance of reporting abuse, misuse or access to inappropriatematerials and know how todoso
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good online safety practicewhen 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

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

E- safety should be taught in all year groups, covering age-appropriate issues. Useful online safety programmesinclude:

- Barnet and LGfL e-Safety and e-literacy Framework for EYFS-Y6 (www. safety.lgfl.net)
- Childnet –http://www.childnet.com/
- http://www.kidsmart.org.uk/
- CEOP - Think U Know (www.thinkuknow.co.uk/)
- CBBC Stay Safe - http://www.bbc.co.uk/cbbc/topics/stay-safe

Parents/Carers

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

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

Policy Statements

Education – pupils - E -Safety curriculum

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

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

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site/page may have a particular bias or purpose andto develop skills to recognise what that may be;
- [for older pupils] to understand how search engines work and to understand that thisaffects theresults theysee at thetop of thelistings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;

- to understand why on-line 'friends' may not be who they say they are and to understand should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure theyhaveturned-onprivacysettings;
- to understand why they must not post pictures or videos of others without their permission;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacheror trustedstaffmember,or an organisationsuchas Childlineor the CLICK CEOP button.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectivesforspecificcurriculumareas.
- Will remind students about their responsibilities through an end-user Acceptable UsePolicy which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitablematerialthatisfoundininternetsearches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person)can temporarily remove those sites from the filter edit list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Online safety Rules

Children at Osidge will follow the rules below to embed online safety:

- Ask permission before using the Internet.
- Only use websites that an adult has chosen.
- Tell an adult if we see anything we are uncomfortable with.
- Immediately close any webpage we not sure about.
- Only e-mail people an adult has approved.
- Only send e-mails that are polite and friendly.
- Never give out personal information or passwords.
- Never arrange to meet anyone we don't know.
- Do not open e-mails sent by anyone we don't know.
- DonotuseInternetchatrooms

Education –parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essentialroleintheeducationoftheirchildrenandinthemonitoring/regulationofthe children's on-line behaviours.Parentsmayunderestimatehow often childrenandyoung peoplecomeacrosspotentially harmfulandinappropriatematerialontheinternetandmaybeunsure abouthow torespond.

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

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

Education & Training – Staff / Volunteers

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

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

Training – Governors

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

- Attendance at training provided by the Local Authority/National Governors Associationor other relevant organisation
- Participation in school training/information sessions for staff

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private

E-mail

This school:

- Provides staff with an email account for their professional use, *LGfL Staffmail* and makes clear personal emails should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained andup to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to thePolice.
- Knowsthatspam,phishingandvirusattachmentscanmakeemailsdangerous.Weusea numberofLGfL-providedtechnologiestohelpprotectusersandsystemsintheschool, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

School website

- The Head Teacher takes overall responsibility to ensure that the website content isaccurate 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, wecreditthe sources usedand stateclearlytheauthor'sidentityorstatus;
- The point of contact on the web site is the school address, telephone number and school officee-mail.
- Photographs of children published on the school website 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 websit

Mobile Phones/ Personal Devices

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

At Osidge School (In line with our Acceptable use agreement) staff must not bring in their own iPadsor laptopsforuseinschool.

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) andhandedintotheschoolofficetobelockedawayuntiltheendoftheschooldaywhenthey canbe collected.

Staff members may only use their phones during school break times, and in the staffroom. It is not permittedforstafftousetheirmobilephonein thevicinity of children. All visitors are requestedto keeptheirphonesonsilent,andmustnotusetheirphoneinthevicinityof children.

Staff personal mobile phones will only be used during lessons with permission from the Head Teacher.

Where staff members are required to use a mobile phone for school duties, for instance, in case of emergency during off-site activities, or for contacting students or parents, they should use their own deviceandhide(byinputting141)theirownmobilenumberforconfidentiality purposes.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

  - Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Those images should only be taken on school equipment; the personalequipmentof staff shouldnot be used for suchpurposes.(includingmobilephones)

- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school intodisrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefullyand will complywith good practiceguidance on the useof such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- We gain parental/carer permission for use of digital photographs or video involving their childaspartoftheschoolagreementformwhentheirdaughter/sonjoinstheschool. This agreement will cover the publication of images on the school website; outside of school: andanyworktobepublishedoutsideofschool.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- Photographs will only be stored off site on password protected PCs by the HeadTeacher and website administrator.

Data Protection

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

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

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it wascollected for.
- Every effort will be made to ensure that data held is accurate, up to date andthat inaccuracies are correctedwithout unnecessarydelay.
- All personal data will be fairlyobtained in accordance with the "PrivacyNotice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data ProtectionAct (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners(IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk

incidents

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner'sOffice

Staff must ensure that they:

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

Technical solutions

- We require staff to log-out of systems when leaving their computer
- We use encrypted flash sticks and EYFS laptops if any member of staff has to take any sensitive informationoffsite.
- WeusetheDfES2SsitetosecurelytransferCTFpupildatafilestootherschools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use LGfL's USO FX to transfer other data to schools in London and the Local Authority such as reports of children.
- We use the LGfL secure data transfer system, USO Auto Update, for creation of online user accounts foraccess to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets or in alockable storage area.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data ,is disposed of properly
- Paper based sensitive information is shredded onsite in small amounts or larger amounts are collected by secure data disposal service.

Technical – infrastructure / equipment, filtering and monitoring

Theschoolwillberesponsibleforensuringthattheschoolinfrastructure/ network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effectiveincarryingouttheironline safetyresponsibilities:

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

Network Management

This school:

- Uses individual, audited log-ins for all users - the London USO system
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies
- Storage of all data within the school will conform to the UK data protection requirements
- We use the London Grid for Learning's Unified Sign-On(USO)system for username and passwords
- Makesclearthatnooneshouldlogonasanotheruserandmakesclearthatpupilsshould neverbeallowedtolog-onoruseteacherandstaffloginsasthesehavefarlesssecurity restrictionsand inappropriateuse 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 logoff when they have finished working or are leaving the computer they are working on.
- Makesclearthatstaffareresponsibleforensuringthatanycomputerorlaptoploanedto them by the school, is used solely to support their professional responsibilities and that they notify the school of any" significant personal use" as defined by HM Revenue & Customs.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g.technical supportor MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Providespupilsandstaffwithaccesstocontentandresourcesthroughtheapproved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Related Policies:

Safeguarding and Child Protection Policy

Signature: Jen Brodkin	Head Teacher	Date: September 2020
Signature: Has Mahir	Chair of Governors	Date: September 2020

Date for Policy Review: September 2021