IT Information and Security Policy	Name of School	Hallsville primary Scott Wilkie primary
	Review Date	December 2021
	Date of next Review	December 2022
	Who reviewed this Policy?	Keri Edge – Executive Headteacher Nigel Mark – ICT Network Manager Andrea Perry – Computing Lead Rianna Lewis - Computing Lead Steve Cox – Education Consultant

IT Information and Security Policy - Managing the Internet Safely

Within all trust schools:

- The Executive Head Teacher is the Senior Information Risk Officer (SIRO).
- NPW is our Data Protection Officer(DPO) dpo@npw.uk.com with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners) as outlined in the schools Data Protection Policy. We have listed the information and information asset owners <in a secure G Suite spreadsheet>.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record. There is a spreadsheet document stored on the trusts Google G Suite domain.
- We ensure ALL the following school stakeholders work in alignment with our Acceptable Use Agreement.
    - staff
    - governors
    - pupils
    - parents
    - volunteers
- In order to access digital devices belonging to the school systems are set up so that users must confirm that they have read and understood our Acceptable Use Policy. This is refreshed at least once per month and makes clear all responsibilities and expectations with regard to data security.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use complex passwords.

- We require staff to change their passwords every 90 days.
- We require that any Protected and Restricted material must be encrypted if the material is to be removed from the school, and limit such data removal.
- School staff who set up usernames and passwords for e-mail, network access, Learning Platform and online Services access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Hallsville and Scott Wilkie Primary School:

- Have the educational filtered secure broadband connectivity through the London Grid for Learning (LGfL) and so connects to the 'private' National Education Network;
- Has its own dedicated firewall, with regular intrusion detection checks being undertaken by the LGfL.
- Make use of the Microsoft Windows Server Update Services (WSUS) to ensure that servers, PCs and laptops receive the latest security updates and hotfixes automatically.
- Uses Mobile Device Management (MDM) software to monitor the status of mobile devices, to ensure they remain up to date and complaint with restriction and security policies.
- Has the ability to remotely lock and erase portable devices in the event of loss or theft.
- Uses the LGfL Netsweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, extremist websites/materials, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged with Newham Partnership Working's (NPW) web development team who manage the schools' web filtering.
- Uses LGfL AutoUpdate for creation of online user accounts for access to broadband services.
- Uses DfE approved cloud storage solutions (Google Drive).
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students / role of staff member.
- Uses security time-outs on user-level Internet filtering access. Staff members are required to re-authenticate onto the system every 30 minutes
- Uses security time outs to also lock workstations in use by staff members that have been inactive for 5 minutes.
- Ensures the network is healthy through use of Sophos anti-virus software (from LGfL) and the network set-up so staff and pupils are unable launch or run unapproved executable files.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock back-up storage devices tapes in a secure, cabinet. Back-ups are encrypted using Microsoft Bitlocker technology. No back-up storages devices leave the site.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our admin and curriculum servers.
- 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.
- Uses LA approved USO FX to send personal data over the Internet and uses encrypted devices and secure remote access (provided by the LGfL RAv3 service) where staff need to

access personal level data off-site. Staff members are required to use 2-factor authentication to use the remote access service.

- Uses 'Pop Up blocking' technology to help filter advertisement and age inappropriate material when using the Internet**.**
- Blocks all known chat rooms and social networking sites except those that are part of an educational network or the Fronter Managed Learning Environment;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with pupils*; Uses Londonmail with students as this has email content control and the address does not identify the student or school;
- Provides staff with a *LGfL Staffmail* email account for their professional use, and makes clear that personal email should be through a separate account;
- Uses teacher 'remote' management control tools (Impero) for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
- Has additional local network auditing software installed;
- Works in partnership with NPW to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Works in partnership with NPW to ensure that it is up to date with LGfL services and policies;
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- We store any Protect and Restricted written material in lockable storage cabinets.
- Paper based sensitive information is shredded, using a cross-cut shredder.

Policy and procedures:

The trust schools:

- Are vigilant in their supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Staff can access the school WiFi via their own devices as long as they:
    1. Are school staff and have signed the schools Acceptable Use Policy (AUP)
    2. Have an active individual, audited log-in from the LGfL USO system

  Additionally, guests and visitors to the school can access the school WiFi as long as they:

    1. Are a member of staff within any LGfL connected school in the LA.
    2. Have an active individual, audited log-in from the LGfL USO system.
    3. Are approved by the head teacher and ICT Team who will issue a temporary access code usually for a period of 8 hours.

  Users connected to the 'GUEST' network will only be able to access the internet and will not be able to access any resources located in the school, such as printers or servers.

All internet traffic on the WiFi network is still monitored and filtered by LGfL Netsweeper filtering system filtering system.

- Ensures pupils only publish within the appropriately secure school's learning environment, such as google drive, Purple Mash, J2E etc
- Requires staff to preview websites and videos before use where not previously viewed or cached. The school allows access to YouTube as a resource, but it is only accessible to:
    1. School staff that have signed the school Acceptable Use Policy (AUP)
    2. Have an active individual, audited log-in from the LGfL USO system
    3. Staff members have to re-verify their credentials with the Netsweeper filtering system every 30 minutes.
- Encourages use of the school's cloud based platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using search engines, with appropriate filtering mechanisms in place to ensure removal of inappropriate content, where more open Internet searching is required; eg google
- Is vigilant when conducting image searches with pupils. Searches should be conducted on small screens (the Interactive Whiteboard should be frozen or turned off) and where possible searches are completed prior to the lesson.
- Informs users that Internet use is monitored;
- Informs staff that that they must report any failure of the filtering systems directly to the ICT Coordinator, or ICT Network Manager. The ICT Coordinator, ICT Network Manager escalates as appropriate to the NPW web development team as necessary;
- Requires pupils to individually sign an e-safety agreement form which is fully explained and used as part of the teaching programme and keeps a copy on file;
- Requires all staff to sign an acceptable use policy agreement form and keeps a copy on file.
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides eSafety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and LA.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils what to do if they find inappropriate web material i.e. click on windows key & 'D' and report to the class teacher or responsible adult.

- Informs staff what to do if they find inappropriate web material i.e. to click on windows key & 'D'/ switch off monitor / and report the URL to the ICT Coordinator or ICT Network Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, which is aligned with the Education For A Connected World framework. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - 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 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music or video files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - 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; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an Acceptable Use Policy which every student will sign and will be displayed throughout the school.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures that staff understand the British Board of Film Classification (BBFC) rating system for videos, and are aware that some online content is now rated by the BBFC using the same criteria guidelines (e.g. UK produced music videos, available on sites like YouTube)
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection e.g. use of USOFX;
- Makes training available annually to staff on the e-safety education program;
- Provides, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.
- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behavior are made clear
    - Information leaflets; in school newsletters; on the school web site, on the MLE;
    - demonstrations, practical sessions held at school;
    - distribution of online Safety materials for parents;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.