On-line Safety Policy

September 2023

Next review: September 2024

Contents

1. Introduction and overview
- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

2. Education and Curriculum
- Pupil on-line safety curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident management

4. Managing the ICT infrastructure
- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data security
- Management Information System access
- Data transfer

6. Equipment and Digital Content
- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:
1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Parents & on behalf of their child)
3. Protocol for responding to incidents of misuse
4. Reporting Log

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 Oliver Thomas Nursery School and Children's Centre with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Oliver Thomas Nursery School and Children's Centre
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school and children's centre 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
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

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

Conduct privacy issues, including disclosure of personal information

- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)

- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope (from SWGfL)
This policy applies to all members of Oliver Thomas Nursery School and Children's Centre community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Oliver Thomas Nursery School and Children's Centre

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for on-line 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 on-line safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious on-line safety incident. • To receive regular monitoring reports from the on-line safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

Role	Key Responsibilities

Head Teacher is the on-line-Safety Co-ordinator as she is the Designated Child Protection Lead. The on-line safety aspect of this role is supported by the School Business Manager	• takes day to day responsibility for on-line safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that on-line safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an on-line safety incident
	• To ensure that an on-line safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in on-line safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media
	• To oversee the delivery of the on-line safety element of the Computing curriculum

Governors / On-line safety governor: Justin Placide	• To ensure that the school follows all current on-line safety advice to keep the children and staff safe
	• To approve the on-line safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about on-line safety incidents and monitoring reports. A member of the Governing Body has taken on the role of on-line safety Governor: Justin Placide
	• To support the school in encouraging parents and the wider community to become engaged in on-line safety activities
	• The role of the on-line safety Governor will include:
	  • regular review with the on-line safety Co-ordinator / Officer (including
	  on-line safety incident logs, filtering / change control logs)

Network Manager/technician – this is the NPW support technician: Nick Bates	• To report any on-line safety related issues that arises, to the on-line safety coordinator. • 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 ICT system

Role	Key Responsibilities
	• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's on-line safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the network including MLE/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher 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 on-line-security and technical procedures
LEARNING PLATFORM Leader (MLE) – this is the LA lead for ICT	• To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected
School Business Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
ICT technician ie who is the LGfL Nominated contact: Nick Bates	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
Teachers	• To embed *on-line* safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's on-line safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of on-line-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 • To report any suspected misuse or problem to the on-line safety coordinator • To maintain an awareness of current on-line safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

Role	Key Responsibilities
	• 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.
Parent Engagement Lead	• Educating Parents and raising awareness as instructed by Head or SLT
Parents/carers	• to support the school in promoting on-line 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
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
How the policy will be communicated to staff/pupils/community/governors 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 pupils (as necessary for visiting students)
- Acceptable use agreements to be issued to whole school community, usually on entry to the school and shared with parents where necessary e.g. parent programmes
- Policy shared and ratified by the governing board

Handling complaints:

- The school will take all reasonable precautions to ensure on-line 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 are given information about infringements in use and possible sanctions. Sanctions available include:
    - Interview by Headteacher or member of SLT;
    - referral to LA / Police
    - disciplinary action.

- Any complaint about staff misuse is referred to the Headteacher. If the complaint is against the Head Teacher the Chair of Governors should be contacted.

- Complaints of cyberbullying are dealt with by the Headteacher. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The on-line safety policy is referenced from within other school policies including Safeguarding and child protection policy, Behaviour policy, GDPR Data Protection Policy & the Social Media policy.

- The school has an on-line safety coordinator (currently the Head Teacher) who will be responsible for document ownership, review and updates.
- The on-line safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The on-line safety policy has been written by the school on-line safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school on-line and safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Even very young children are accessing the internet via phones, tablets and computers, through web browsers and apps. We provide regular e-safety workshops for parents and also provide information in our newsletters about keeping children safe on-line. This includes a strong focus on the use of parental controls on devices to ensure that children do not accidentally access unsuitable material online.

In the nursery school, children will access some material online with support e.g. searching for information about a topic of interest, like dinosaurs. This is carefully supervised and we teach children a range of skills appropriate to their age and experience to keep safe on-line. Staff will model safe and responsible behaviour in their own use of technology during sessions. Staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

Staff and governor training

This school and children's centre

- Ensures staff and governors know 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 and governors on on-line safety issues and the school's on-line safety education program through induction processes, annual appraisal discussions; training in the CC; whole staff training
- Provides, as part of the induction process, all new staff and governors [including those on university/college placement and work experience] with information and guidance on the on-line safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school and children's centre

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information leaflets; in school newsletters; on the school website;
    - demonstrations, practical sessions held at school;
    - suggestions for safe internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school and children's centre, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences

Staff

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the on-line safety acceptable use agreement form at time of their child's entry to the school

Incident Management

In this school and children's centre:

- there is strict monitoring and application of the on-line-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 and regional broadband grid, UK Safer Internet Centre helpline) in dealing with on-line safety issues
- monitoring and reporting of on-line safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- parents / carers are specifically informed of on-line 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. Managing the ICT infrastructure

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

This school and children's centre:

- 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 or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- 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, as far as is reasonable
- Ensures all staff and parents have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures staff only publish within an appropriately secure environment : the school's managed learning environment through LGfL
- Requires staff to preview websites before use [where not previously viewed or cached] Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , 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 that that they must report any failure of the filtering systems directly to the School Business Manager. The SBM logs or escalates as appropriate to the Technical service provider 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 – through staff meetings and training
- 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 and children's centre
  - Uses individual, audited log-ins for all users - the London USO system;
  - Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful through ITASS;
  - Ensures the ITASS and NPW Systems network manage 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

    Staff using mobile technology, where storage of data is online, will conform to the **EU data protection directive** where storage is hosted within the EU.

To ensure the network is used safely, this school and children's centre

- Ensures staff read and sign that they have understood the school's on-line safety Policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different / use the same 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;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- Has set-up the network with a shared work area for staff. Staff 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. [Users needing access to secure data are timed out after at least 10 minutes and have to re-enter their username and password to re-enter the network;
- 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 and we also automatically switch off all computers at 6 pm to save energy;
- 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 staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; this includes Borough email or Intranet; finance system, Personnel system etc
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- 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 for example SEN coordinator - SEN data
- 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: for example LGfL e mail
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support,

- provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of MIS 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 /appropriate 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 ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff to use STRONG passwords for access into our MIS system
- We require staff to change their passwords into the MIS, LGfL USO admin site every 90 days

E-mail

This school

- Provides staff and governors with an email account for their professional use, London Staffmail 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. We use anonymous or group e-mail addresses, for example **info@schoolname.la.sch.uk / head@schoolname.la.sch.uk**

- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- **Pupils at Oliver Thomas do not have individual access to LGFL Mail.**

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX; egress.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;

- All staff sign our LA / school Agreement Form AUP to say they have read and understood the on-line safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School and children's centre website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: these are SLT or delegated authorised website manager

- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the setting's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@oliverthomas.newham.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached without permission;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.
- Compliancy is checked by the governing board.

Learning platform

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

Social networking (see also Social Media policy)

- Teachers are instructed not to run social network spaces for parent use on a personal basis or to open up their own spaces to parents of their pupils, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy. School staff will ensure that in private use:
  - No reference should be made in social media to pupils, parents / carers or school staff
  - They do not engage in online discussion on personal matters relating to members of the school community
  - Personal opinions should not be attributed to the school or local authority
  - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses the LGfL supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV (see also the CCTV policy)

- We have CCTV in the outside site as part of our site surveillance for intruder identification. We will not reveal any recordings (*retained by the Support Provider for 7 days*), without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer (see also the Data Protection policy)

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are currently held by School Business Manager on the W drive. All assets are named as property of the school.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record on the Head Teacher's personal drive that the School Business Manager can also access.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form or in the case of governors, have read the acceptable use form. We have a system so we know who has signed.
    - staff,
    - pupils (referring to secondary school students or volunteers or student placements)
    - parents (including parent programmes)

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- 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.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs this is currently the S drive. Office staff can access the W drive. .
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the Atomwide site to securely transfer CTF pupil data files to the LA and other schools.

- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use <LGfL's USO FX> to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in <lockable storage cabinets in a lockable storage area>.
- All servers are in the main reception area in a lockable location managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network, admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and <get a certificate of secure deletion for any server that once contained personal data- as recommended by NPW
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is <shredded, using cross cut shredder.
- We are using secure file deletion software.

6. Equipment and Digital Content

- I pads (used for registration) and for videoing learning, school cameras and laptops and school educational visit mobile phone can be used off site with the authorisation of a member of SLT for educational purposes.

Personal mobile phones and mobile devices (see also Mobile Phone policy)

- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms.
- Mobile phones brought into school are entirely at the staff member, students' & 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 and volunteer mobile phones which are brought into school must be turned off or placed on silent and stored out of sight on arrival at school. 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 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.

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.
- Staffs 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 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 consent 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;
- Staff and parents 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.
- Parents and staff 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 that reveals the identify of others and their location, such as house number, street name or school where appropriate. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to **The Waste Electrical and Electronic Equipment Regulations 2006** and/or **The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007**. **Further information** can be found on the Environment Agency website.

Appendix 1 Staff & Volunteer Acceptable Use Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school and children's centre systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school and children's centre will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person, the head teacher or DSL on site.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. (Please see mobile phone policy)
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ----------
Signed: ----------
Date: ----------

Appendix 2 Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school and children's centre will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work and sign on behalf of their child.

Permission Form

Parent/Carers Name: .....

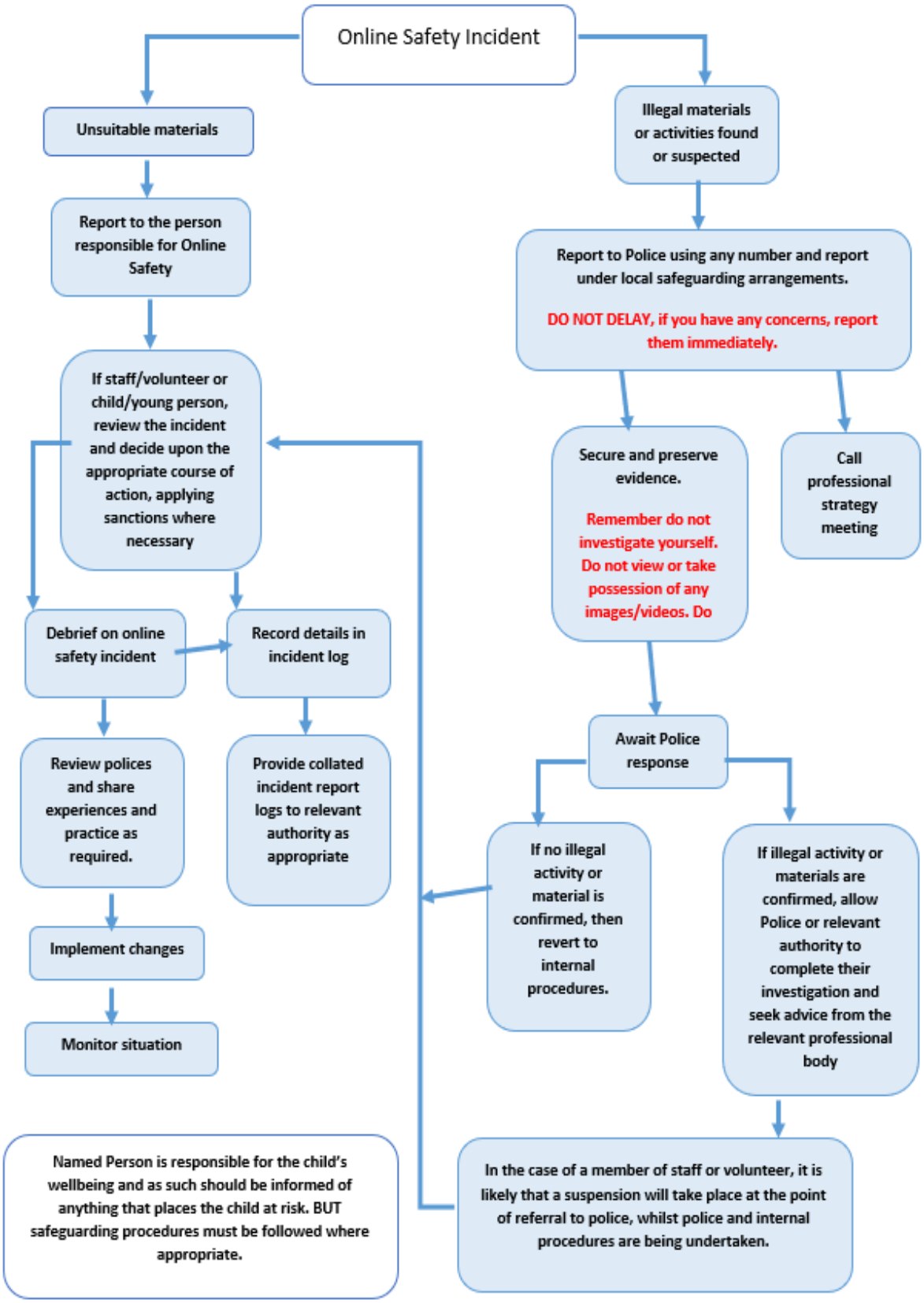
Learner Name: .....

1. As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school and children's centre.
2. I understand that the school and children's centre will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
3. I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
4. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....date.....

This form will be held in print and stored in your child's registration file. Senior leaders and key people will have access to this form. The form will be stored for as long as your child attends Oliver Thomas nursery school and / or children's centre and will be destroyed once they leave.

Appendix 3 Responding to incidents of misuse – flow chart



Appendix 4 Reporting Log

Reporting Log

Group: _____

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Oliver Thomas Nursery School Children's Centre