Online Safety Policy
Oakthorpe Primary School

Reviewed by:	M. Wood	**Date:** January 2021
Approved by:	Teaching and Learning Committee	
Next review due by:	January 2024	

Contents

Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff in each school.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community. Have clear structures to deal with online abuse such as online bullying.
- 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 community can be summarised as follows:

- Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

- Failure to comply with GDPR regulations

Scope

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

Roles and responsibilities-

Headteacher

- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Enfield Safeguarding Partnership guidance
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.
- To take overall responsibility for online safety provision
- To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling
- To ensure the school uses appropriate IT systems and services including, filtered internet Service, e.g. LGfL services
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- To be aware of procedures to be followed in the event of a serious online safety incident
- Ensure suitable 'risk assessments' undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures
- To ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- To ensure school website includes relevant information.

PSHE Team, Designated Safeguarding Lead (DSL) and Computing Lead

- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy
- Promote an awareness and commitment to online safety throughout the school community
- Ensure that online safety education is embedded within the curriculum
- Liaise with school technical staff where appropriate
- To communicate regularly with SLT and the designated child protection Governor 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 online safety incident
- To ensure that online safety incidents are logged as a safeguarding incident
- Facilitate training and advice for all staff
- Oversee any pupil surveys / pupil feedback on online safety issues
- Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns
- Attend relevant training and update sessions

Governing Body

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To support the school in encouraging parents and the wider community to become engaged in online safety activities
- For the Child Protection Governor to meet with the team who lead online safety and report back to the Governing Body on the schools processes and procedures

Computing Curriculum Leader

- To oversee the delivery of the online safety element of the Computing curriculum

ICT Technical Team

- To report online safety related issues that come to their attention, to the DSL
- To manage the school's computer systems, ensuring
  - school password policy is strictly adhered to.
  - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)
  - 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
- That they keep up to date with the potential viruses/online safety issues
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Computing Lead/Headteacher
- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the school's online security and technical procedures
- To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant

Data and Information (Asset Owner) Manager (IAO)

- To ensure that the data they manage is accurate and up-to-date
- Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- The School must be registered with Information Commissioner

All staff, volunteers and contractors

- To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates annually. The AUA is signed by new staff on induction.
- To report any suspected misuse or problem to the Computing Lead/DSL/Headteacher
- Maintain awareness of current online safety issues and through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset

Pupils

- Read, understand, sign and adhere to the ‘Using the Internet Safely Agreement’
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and know that Oakthorpe’s online safety policy covers actions out of school
- To contribute to any ‘pupil voice’ / surveys that gathers information of their online experiences

Parents/carers

- To read, understand and promote the school’s ‘Using the Internet Safely Agreement’with their child/ren
- To consult with the school if they have any concerns about their children’s use of technology
- To support the school in promoting online safety and endorse the School’s Agreements which includes the pupils’ use of the Internet and the school’s use of photographic and video images

External groups including Parent groups (e.g. Friends of Oakthorpe)

- Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school
- To support the school in promoting online safety
- To model safe, responsible and positive behaviours in their own use of technology.

Communication:

- The policy will be communicated to Staff/Pupils/Governors /Parents and the community in the following ways:
- School website
- On the shared drive for staff
- Policy to be part of school induction for new staff
- Regular updates and training on online safety for all staff
- Use of the school’s IT equipment is part of the Staff Code of Conduct
- ‘Using the Internet Sensibly agreement for children – Online Safety Policy 2021’
- ‘Acceptable Use of Digital Technologies Agreement for Staff - Online Safety Policy 2021’

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety
- Staff and pupils are given information about infringements in use and possible sanctions
- Designated Safeguarding Lead (DSL) to act as the first point of contact for any incident. Any suspected online risk or infringement must be reported that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer)

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:
There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people. When assessing the risks the following should be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then the school may decide to respond to the incident without involving the police or children's social care (the school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

- This policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy. Staff Code of Conduct)
- There is widespread ownership of the policy and it has been agreed by the Governing Body. All amendments will be disseminated to all members of staff and pupils

Education and Curriculum

Pupil online safety curriculum

Oakthorpe Primary School:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Plan online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind pupils about their responsibilities through the pupil 'Using the Internet Sensibly agreement for children – Online Safety Policy 2021'
- Ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments

Staff and governor training

Oakthorpe Primary School will:

- Make regular training available to staff on online safety issues and the school's online safety education program;
- Provide, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on online safety procedures and the school's 'Acceptable Use of Digital Technologies Agreement for Staff - Online Safety Policy 2020' and the Staff Code of Conduct

Parent awareness and training

Oakthorpe Primary School will:

- Provide induction for parents which includes online safety;
- Run a rolling programme of online safety advice, guidance and training for parents

Expected Conduct and Incident Management

Expected conduct

All Users:

- Are responsible for using the school IT and communication systems in accordance with the relevant policies;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Know and understand school policies on the use of mobile and hand held devices including cameras;

Parents/Carers:

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the ‘Working in Partnership Agreement’ and ‘Acceptable Use Agreement;
- Should know and understand what the school’s ‘rules of appropriate use for the whole school community’ are and what sanctions result from misuse

Staff, volunteers and contractors:

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Incident Management

- There is strict monitoring and application of the online safety and a differentiated and appropriate range of sanctions;
- All members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA

Managing IT and Communication Systems

Internet access, security (virus protection) and filtering

Oakthorpe Primary School

- Informs all users that Internet/email use is monitored;
- Ensures educational filtered secure broadband connectivity through the LGfL;
- Use the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Use USO user-level filtering where relevant;
- Ensure network health through use of Sophos anti-virus software (from LGfL);
  Use DfE, LA or LGfL approved systems including LGfL USO email to send 'protect-level' (sensitive personal) data
- Use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Work in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students

Network management (user access, backup)

Oakthorpe Primary School will:

- Use individual, audited log-ins for all users - the LGfL USO system;
- Use guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Use teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Ensure 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;
- Have daily back-up of school data (admin and curriculum);
- Use secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Store of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU

To ensure the network is used safely Oakthorpe Primary School will:

- Ensure staff read the school's on-line policy and sign the 'Acceptable Use of Digital Technologies Agreement for Staff - Online Safety Policy 2021' . Following this, they are set-up with Internet, email access and network access. We also provide individual usernames and passwords for access to our school's network;
- Ensure pupils have their own unique username and password which gives them access to the Internet and other services;
- Make 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;
- 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;
- Require all users to log off when they have finished working or are leaving the computer unattended;
- Ensure all equipment owned by the school and/or connected to the network has up to date virus protection;

- Make clear to staff that they are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Make clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintain equipment to ensure Health and Safety is followed;
- Ensure that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Have a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Use secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensure 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);

Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.

All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Password policy

- Oakthorpe will make it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private
- We require staff to use STRONG passwords
- We require staff using critical systems to use two factor authentication

E-mail

Oakthorpe Primary School will:

- Provide staff with an email account for their professional use, London Staffmail /Gmail (Oakthorpe.net) and makes clear personal email should be through a separate account;
- Use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses.
- Contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Ensure that email accounts are maintained and up to date
- 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

Pupils:

- We use LGfL pupil email system and Google Classroom which are intentionally 'anonymised' for pupil protection
- Pupils are taught about the online safety and 'etiquette' of using e-mail both in school and at home through the 'Using the Internet Sensibly agreement for children – Online Safety Policy 2020'.

Staff:

- Staff can only use the Google Education or LGfL email systems on the school system
- Staff will use Google Education or LGfL email systems for professional purposes
- Access in school to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption

School website

- The Headteacher, supported by the Governing Body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website or Cloud Environments
- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate
- Teachers are instructed not to run social network spaces for pupils use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communication School staff will ensure that in private use:
- No reference should be made in social media to students/pupils, parents/carers or school staff; School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute; Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- Pupils are required to sign and follow our [age appropriate] 'Using the Internet Sensibly agreement for children – Online Safety Policy 2021'.

Parents:

- Parents are reminded about social networking risks and protocols through our Home School Agreement and additional communications materials when required
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of Oakthorpe Primary School and 2Schools Consortium (Oakthorpe's Initial Teacher Training Provision) and will not use for any other purposes.

Data Security: Management Information System Access and Data Transfer

Strategic and operational practices

Oakthorpe Primary School will ensure:

- The Headteacher and staff follow the advice of the LA Data Controller
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- Staff know who to report any incidents where data protection may have been compromised
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on Google Drive to store sensitive files
- All servers are in lockable locations and managed by DBS-checked staff
- 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
- 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
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices 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
- All pupil mobile devices will be handed in to classteachers or the school office should they be brought into school and must be turned off
- The Bluetooth or similar function of pupil mobile device should be switched off at all times and not be used to send images or files to other mobile devices
- All visitors are requested to keep their phones on silent
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device
- PIN access to the device must always be known by the network manager

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom
- PIN access to the device must always be known by the network manager
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Pupils' use of personal devices

- The school strongly advises that pupil mobile phones and devices should not be brought into school The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office.
- Mobile devices will be released to parents or carers in accordance with the school policy
- Phones and devices must not be taken into examinations.
- Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances
- 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
- 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 and then report the incident with the Headteacher /Designated Officer.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- Staff mobiles devices may be searched at any time as part of routine monitoring
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times

- Staff members may use their phones during school break times in areas where children are not present
- 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
- If a member of staff breaches the school policy, then disciplinary action may be taken

Digital images and video

Oakthorpe Primary School:

- Gains parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually);
- 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 of Digital Technologies Agreement for Staff - Online Safety Policy 2020'and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- Block/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying and abuse

Remote working

- Staff working at home will ensure that they ensure that their display screen equipment is safely organised https://openerg.com/dse/setup.html
- Staff who need to speak to parents of children during remote working, e.g. for safeguarding purposes will hide their number using 141. If staff have concerns they will record the conversation either on safeguard or on a meeting with parents sheet and forward details of the conversation to the Head teacher
- Staff will not contact parents using individual work emails, personal emails or social media. They will send messages to the SBM / SLT who will send the message to parents using the office@oakthorpe.enfield.sch.uk email address or via scholarpack. Replies from parents will be forwarded to staff.
- Staff can talk to their class on Google classroom and can take part in Google Hangouts but no chats should happen on teacher's private logins.
- During virtual lessons children can use a camera but staff will actively explain to children how to turn off their cameras to support children to be safe online when using other social media platforms.

- Staff will manage communication and notifications carefully to support their work/life balance. Staff are encouraged to use ‘out of office’ and have set hours for meetings and hangouts.
- Teachers will only communicate with students via the school-sanctioned channels, and children will also be told how to expect communications to arrive from their teachers, and to report any communication other than the sanctioned school staff.

Linked policies

1. Child Protection
3. Acceptable Use of Digital Technologies Agreement – Staff, Governors & Volunteers
4. Using the Internet Sensibly agreement for children – Children
5. Staff Code of Conduct / Handbook
6. Remote Learning Policy
7. Data Protection Policy & GDPR Staff Handbook
8. Behaviour Policy
9. Anti-Bullying Policy
10. *DfE (2020) Keeping Children Safe in Education.
11. *DfE (2019) Teaching Online Safety in Schools.
12. *Education for a Connected World cross-curricular digital resilience framework (UKCIS)
13. *Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
14*Sexting guidance from UKCIS
    - o *Overview for all staff
    - o *Full guidance for school DSLs
15. *Prevent Duty Guidance for Schools (DfE and Home Office documents)

Where marked with * the latest version or a template you may use is available at safepolicies.lgfl.net

Appendix 1

Acceptable Use of Digital Technologies Agreement for Staff, Governors and Volunteers

This document covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems. Staff will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

- It is advisable to use the school (LGfL) secure or Google Suite email system or for any school business and where this is not used, I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not browse, download or send material that could be considered offensive to colleagues and will report any potentially dangerous/risky incidents.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will take every precaution to ensure that when I connect any electronic equipment (e.g. USB memory stick) to the school computers/network it is either scanned or if it is a laptop, has up to date virus software.
- Images of pupils will only be used in accordance with our Online safety policy
- I will inform the school if I object to my image being used for school purposes. (i.e. in such locations as the school website.)
- I will use the school's Learning Platform in accordance with school and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to do not compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will only use LA systems in accordance with any corporate policies.

I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action and possibly even dismissal.

User Signature

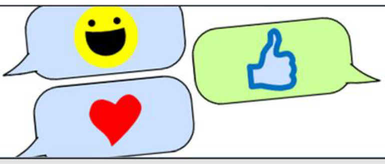
I agree to abide by the school's most recent Acceptable Use of Digital Technologies Policy.
Signature . . . . Date . . . .

Full Name...(printed) Job title. . . . .

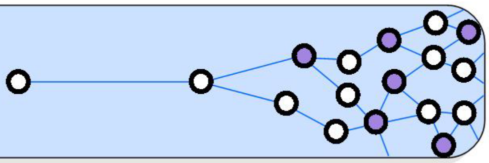
Appendix 2

8 tips to stay safe online

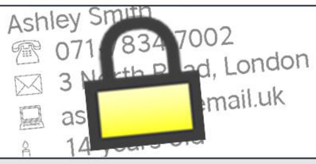
1 Be nice to people online.



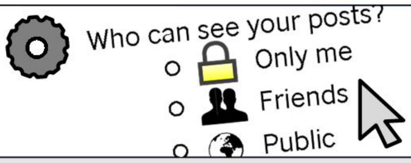
2 Take care with what you share.



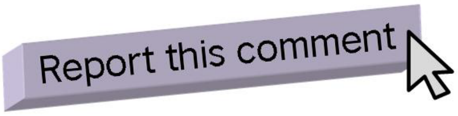
3 Keep personal information private.



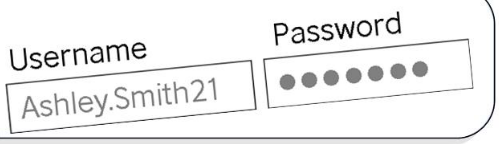
4 Check your privacy settings.



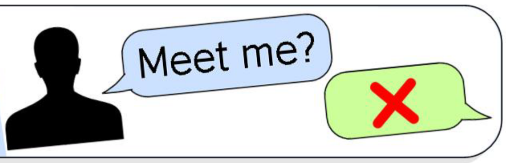
5 Know how to report posts.



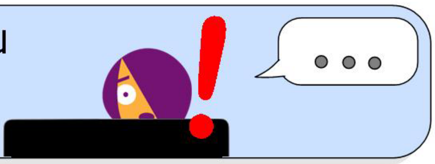
6 Keep your passwords safe.



7 Never meet anyone in person you've only met online.



8 If you see anything online that you don't like or you find upsetting, tell someone you trust.



Appendix 3

LGfL DigiSafe keeping children safe

Using the Internet Safely Agreement

Oakthorpe Primary School

My name is ______________________

To stay **SAFE online and on my devices**: ✓

1. I only **USE** devices or apps, sites or games if a trusted adult says so □
2. I **ASK** for help if I'm stuck or not sure □
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused □
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult □
5. I look out for my **FRIENDS** and tell someone if they need help □
6. I **KNOW** people online aren't always who they say they are □
7. Anything I do online can be shared and might stay online **FOREVER** □
8. I don't keep **~~SECRETS~~** or do **DARES AND CHALLENGES** just because someone tells me I have to □
9. I don't change **CLOTHES** in front of a camera □
10. I always check before **SHARING** personal information □
11. I am **KIND** and polite to everyone □

My trusted adults are:

______________________ **at school**

______________________ **at home**

____

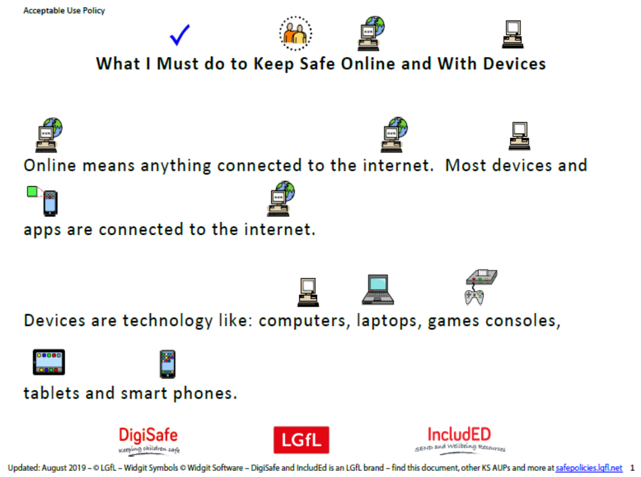
For parents/carers

To find out more about online safety, you can read Oakthorpe Primary School's full Online Safety policy on the website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

You can find support and online safety resources for parents at parentsafe.lgfl.net

Appendix 4

Using the Internet Safely Agreement for children with SEND



Acceptable Use Policy

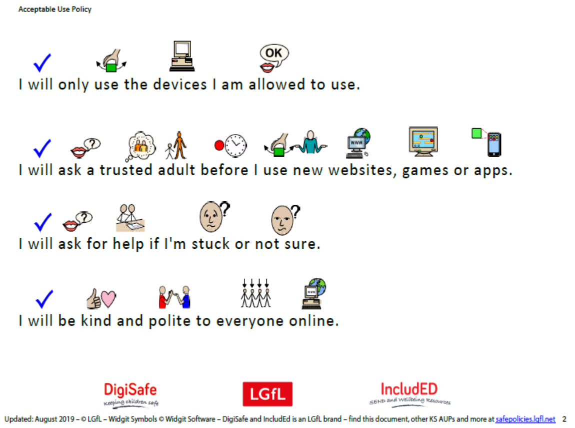
✓ What I Must do to Keep Safe Online and With Devices

Online means anything connected to the internet. Most devices and apps are connected to the internet.

Devices are technology like: computers, laptops, games consoles, tablets and smart phones.

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 1



Acceptable Use Policy

✓ I will only use the devices I am allowed to use.

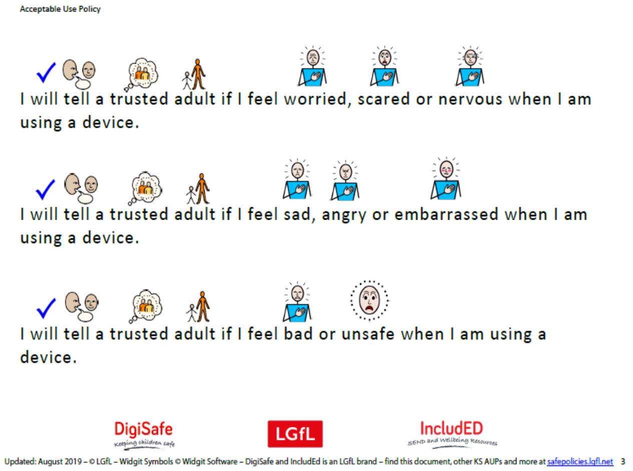
✓ I will ask a trusted adult before I use new websites, games or apps.

✓ I will ask for help if I'm stuck or not sure.

✓ I will be kind and polite to everyone online.

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 2



Acceptable Use Policy

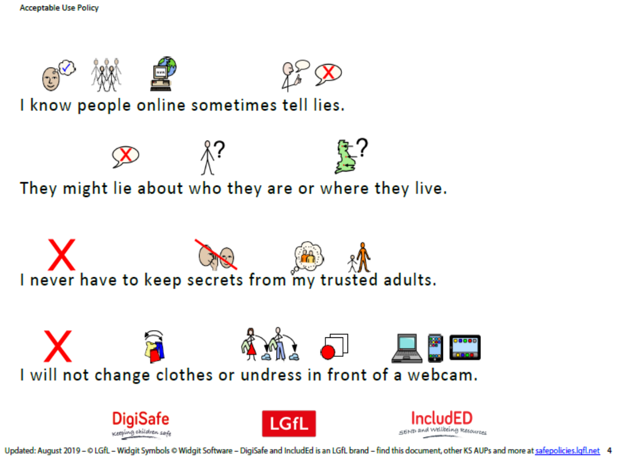
✓ I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.

✓ I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.

✓ I will tell a trusted adult if I feel bad or unsafe when I am using a device.

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 3



Acceptable Use Policy

I know people online sometimes tell lies.

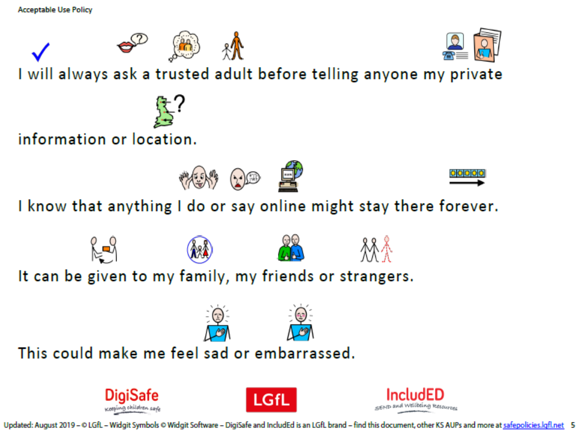
They might lie about who they are or where they live.

✗ I never have to keep secrets from my trusted adults.

✗ I will not change clothes or undress in front of a webcam.

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 4



Acceptable Use Policy

✓ I will always ask a trusted adult before telling anyone my private information or location.

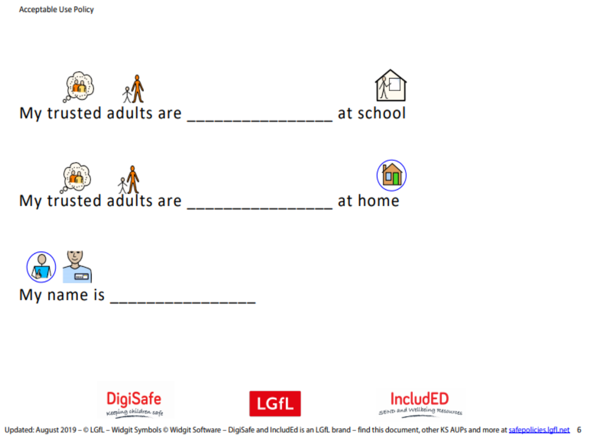
I know that anything I do or say online might stay there forever.

It can be given to my family, my friends or strangers.

This could make me feel sad or embarrassed.

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 5



Acceptable Use Policy

My trusted adults are _______________ at school

My trusted adults are _______________ at home

My name is _______________

DigiSafe Keeping children safe LGfL IncludED SEND and Wellbeing Resources

Updated: August 2019 – © LGfL – Widgit Symbols © Widgit Software – DigiSafe and IncludED is an LGfL brand – find this document, other KS AUPs and more at safepolicies.lgfl.net 6

Appendix 5

Tips for working on a PC or laptop remotely:

- Raise your screen: Make sure your screen is raised so that the top of the screen is at eye level. This can be done using an adjustable laptop stand, a box or some books if necessary.
- Use a separate keyboard and mouse. This enables the laptop screen to be positioned correctly.
- Report pain or discomfort. If you feel discomfort, report it to your line manager as soon as you notice it. In some circumstances, a referral to the Occupational Health Service may be appropriate.
- Adjust your chair height. Your arms should be at right angles, with forearms lightly supported by the work surface. You may need a footrest if your feet are not firmly on the floor.
- Make sure the lower back is well supported Support for your lower back will help encourage good posture. You can use a folded towel to give you more support or consider a back-support cushion if needed.
- Take regular, short breaks: Move around for five or ten minutes every hour, aiming for frequent, short breaks.
    - Consider taking micro-breaks to stretch, move around, change activity by taking a phone call, do some reading or get a drink to avoid prolonged static postures.
    - Take more frequent breaks if your DSE setup is not optimal or if you are experiencing discomfort.

Try to avoid:

- using phones or tablets for a long time,
- sitting on unsupportive seating such as a sofa,
- static postures

Whilst it may seem easier to simply open the laptop and start working without making any adjustments, this can lead to poor posture, which can cause pain and discomfort over time. It is well worth taking a couple of minutes to set up your workstation correctly each time you sit down to work.