Hallfield Primary School

Growing, Learning, Achieving Together

Online Safety Policy

This policy has been created using the LGFL School Online Safety Policy Template. It is part of the school's statutory safeguarding policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview
    - Rationale and Scope
    - Roles and responsibilities
    - How the policy is communicated to staff/pupils/community
    - Handling incidents
    - Reviewing and Monitoring
2. Education and Curriculum
    - Pupil online safety curriculum
    - Staff and governor training
    - Parent awareness and training
3. Expected Conduct and Incident Management
4. Managing the IT Infrastructure and Communication Sytems
    - Internet access, security (virus protection) and filtering
    - Network management (user access, backup)
    - Passwords policy
    - E-mail
    - School website
    - Social networking
    - CCTV
5. Data Security
    - Strategic and operational practices
    - Technical Solutions

6. Equipment and Digital Content

- **Mobile devices**
- **Digital images and video**

Appendices:

A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreement including photo/video permission (Parents)

A3: Acceptable Use Agreements (Pupils – adapted for phase - proforma)

A4: Protocol for responding to online safety incidents/concerns

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 Hallfield Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- 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 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 safety concerns or abuse such as online bullying (noting that these need to be 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 pupils.

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)

Scope

This policy applies to all members of the Hallfield Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) 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 (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, i.e. 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 • To ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Designated Safeguarding Lead • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • 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
Designated Safeguarding Lead (Philip Tomsett) in coordination with the **Online Safety Coordinator** (Zoe Harris)	• To take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • To promote an awareness and commitment to online safety throughout the school community • To ensure that online safety education is embedded within the curriculum • To liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review reported incidents

Role	Key Responsibilities
	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 safeguarding incidents • To facilitate training and advice for all staff • To oversee any pupil surveys/pupil feedback on online safety issues • To liaise with the Local Authority and relevant agencies • To be regularly updated on online safety issues and legislation, and be aware of the potential for serious child protection concerns
Governors / Safeguarding governor (including online safety) (Eloise Newnham)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • To have regular reviews with the Designated Safeguarding Leads (DSLs)
Computing Curriculum Leader (Zoe Harris)	• To oversee the delivery of the online safety element of the computing curriculum • To provide annual training updates and induction for new staff
Network Manager / technician (Turn IT On)	• To report online safety related issues that come to their attention • 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 • To keep up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms is regularly monitored and that any misuse/attempted misuse is reported • 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

Role	Key Responsibilities
Data and Information Asset Owner Managers (IAOs) (Maria Martin)	• To ensure that the data they manage is accurate and up-to-date • To ensure best practice in information management i.e. have appropriate access controls in place and that data is used, transferred and deleted in-line with data protection requirements • To ensure the school is registered with Information Commissioner
LGfL Nominated contact(s) (Maria Martin, Ann Little, Turn IT On)	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities where 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, volunteers and contractors	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy (AUP) on induction and thereafter if any amendments are made • To understand any updates to the AUP • To report any suspected misuse or problem to a DSL • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy • 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 a manager / technician on the last day to log in and allow a factory reset
Pupils	• To read, understand, sign and adhere to the Pupil AUA annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise

Role	Key Responsibilities
	that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' surveys that gather information of their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use 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 Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use Policy prior to using technology or the Internet within school where applicable • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology

Communication

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

- Posted on the school website, circulated by email and available in the staffroom
- Included in the school induction pack for new staff
- Through regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year
- Acceptable use agreements to be issued to members of the school community, on entry to the school
- Annual update training

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 Leads (DSLs) act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to a Designated Safeguarding Lead.

- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the incident is referred to the Chair of Governors.
- In the instance of handling a sexting/nude selfie incident UKCCIS "Sexting in schools and colleges" should be used.

Reviewing and Monitoring Online Safety

The Online Safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy)

- The online safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures 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;
- ensures 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

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;

- provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction information for parents which includes online safety;
- offers online safety advice, guidance and training for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting 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.

Staff, volunteers and contractors who work with children

- 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.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's rules of appropriate use for the whole school community are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy;
- 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.

4. Managing the IT Infrastructure and Communication Systems

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses 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;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works 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)

This school:

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet websites, where useful;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage 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, this school:

- Ensures staff read and sign that they have understood this Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Access to services is through a unique username and password;
- 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;
- Has set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working and lock the computer if they are leaving it computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes 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.
- Maintains equipment to ensure appropriate health and safety standards are met;
- Ensures 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;
- Does 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;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;

- This school uses secure data transfer; this includes 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 Egress and 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

- This school makes it clear that staff and pupils should always keep their passwords private and not share them with others; if a password is compromised the school should be notified immediately.
- Staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private. These are changed every 90 days.
- We recommend staff to use strong passwords.
- Staff are required to change their password for CPOMs every 60 days.
- We require staff using critical systems to use two-factor authentication.

E-mail

This school:

- Provides staff with an email account for their professional use (LGFL Staffmail) and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses, for example office@hallfieldschool.org.uk/or class e-mail addresses.
- 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.
- 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.

Pupils:

- Pupils are taught about online safety and have annual updates.

Staff:

- Staff will use LGfL e-mail systems for professional purposes only.

- Access in school to external personal e mail accounts may be blocked
- 'Protect-level' staff or pupil personal data should be transferred by secure file transfer. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website/blog

- 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 web site 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.

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 student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Any school-approved social networking will adhere to the "three commons" approach (Appendix 2).

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.
- Students are required to sign and follow the age appropriate pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use 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.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information (the Information Asset Owners) are.
- 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 a single central record.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in the asset register.
- 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.
- We are using secure file deletion software.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices) - see also school's Mobile phone Policy

- Mobile devices brought into school are entirely at the staff member, student, parent or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- No child should have a mobile phone in school. Some Year 6 children may bring one to school, with parent's written permission, but they must be given to the site keeper before school and collected at the end of the day as they leave.
- Staff must have their mobile phones on silence/switched off and stored out of children's sight and access.
- Staff must not use their own personal mobiles to take photos of children or give children or parents their own personal numbers.
- Personal mobile devices will not be used during lessons or formal school time.
- Staff members may use their phones during school break times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- 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 will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- If a member of staff breaches the school policy then disciplinary action may be taken.

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 induction 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 Agreement and this includes a clauses regarding taking pictures of pupils;

- If specific pupil photos are used in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- 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 or abuse.

LONDON GRID FOR LEARNING

Appendix 1

	Name of School	**Hallfield Primary School**
	AUA review Date	**April 2019**
	Date of next Review	**April 2020**
	Who reviewed this AUP?	**AS, ZH, MM**

Acceptable Use Agreement: Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.

Hallfield Primary School regularly reviews and updates all AUA documents to ensure that they are consistent with the school's Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I 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.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and/or use of my password(s) and change my password(s) as and when required, including if a password is compromised. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email/Internet/network, other school or Local Authority systems I have access to.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted/shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system, LGFL StaffMail, for any school business.
- I will only use the school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Headteacher, Aaron Sumner.

- I will not download any software or resources from the Internet that could compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drives), to the network that do not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's **Mobile Phone** and **Online Safety** policies on use of mobile phones/devices at school.
- I will only use school approved equipment for any storage, editing or transfer of digital images/videos.
- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital/video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will ensure that any private social networking sites/blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites/tools securely, so as not to compromise my professional role.
- I agree and accept that any electronic equipment 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 only access school resources remotely (such as from home) using the LGfL, Google Drive and school approved system and follow e-security protocols to interact with them.
- 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 report the behaviour of any child I feel may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way.
- I understand that all Internet and network traffic/usage can be logged and this information can be made available to the Head and/or Designated Safeguarding Officer on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any school approved systems I have access to in accordance with their policies.
- I will embed the school's on-line safety/digital literacy/counter extremism procedures into my practice.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety/safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher/School Business Manager)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name ..... (printed)

Hallfield Primary School *regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.*
The Pupil Acceptable Use Agreements are attached to this form for reference.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- IT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs, videos etc., about other children (or staff) at school events, without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe and responsible use of the Internet, online services and digital technology at home. I will inform the school if I have any concerns.

Name of child: _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

Hallfield Primary School's rules for any external use of digital images are:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity (e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian).
- Your child's image being used for presentation purposes around the school (e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators (e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
- In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission (e.g. if your child won a national competition and wanted to be named in local or government literature.

I agree to the school using photographs of my child or including them in video material, as described. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____ Date: ___/___/___

The use of social networking and online media

This school asks its whole community to promote the "three commons" approach to online behaviour:

- Common courtesy
- Common decency
- Common sense

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This may constitute online-bullying and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the reputation of the school, or someone in it, in some way or are deemed as being inappropriate will be managed and responded to appropriately.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments online, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting abuse: thinkuknow.co.uk/parents/

LONDON GRID FOR LEARNING

KS1 Acceptable Use Agreement

Hallfield School



Class _____ Date _____

	✓
I keep **SAFE online** because …	
I **CHECK** it's OK to use a website / game / app.	
I **ASK** for help if I get lost online.	
I **THINK** before I click on things.	
I **KNOW** that online people are really strangers.	
I am **RESPONSIBLE**, so I never share private information.	
I am **KIND** and polite online.	
I **TELL** a trusted adult if I am worried about anything.	











LONDON GRID FOR LEARNING

Hallfield School

KS2 Pupil Online Acceptable Use Agreement

Class _____ **Date** _____

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe and has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions. I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults, if a friend or person I know is being bullied or harassed online, or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons license.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers, but I will always ask my trusted adults for and follow their advice.

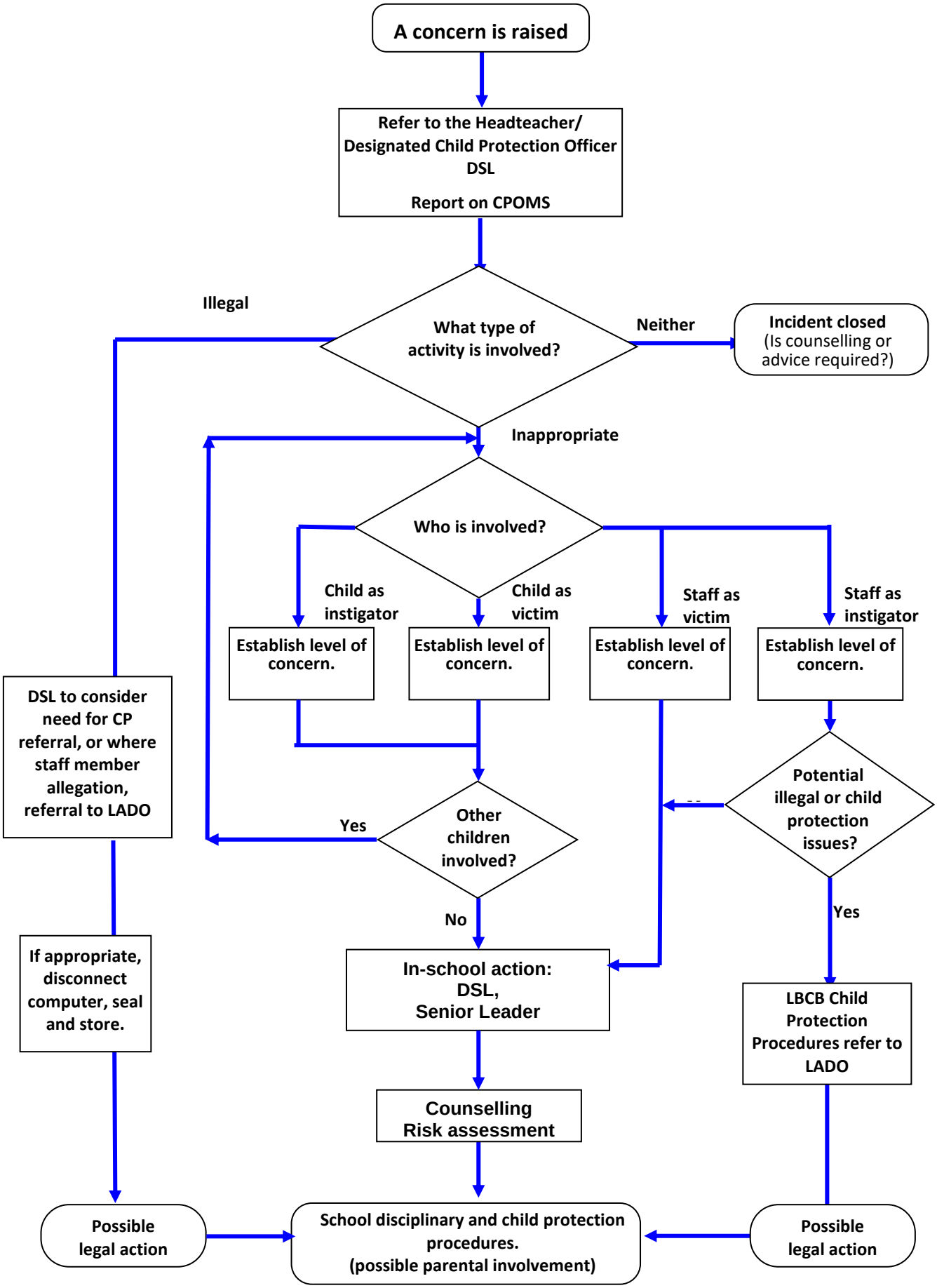
I have read, understood and will follow this agreement.

I know who are my trusted adults are.





What to do if you have an E-safety concern:



Duty LADO: 02076416108 (Local Authority Designated Officer)

Children's Services Area Teams