



## Chalkhill Primary School E-Safety Policy 2024-2025

### Contents

#### 1. Introduction and overview

- Rationale and Scope
- Legislation and Guidance
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

#### 2. Education and Curriculum

- Pupil e-safety Curriculum
- Staff and governor training
- Parent awareness and training

#### 3. Expected Conduct and Incident management

#### 4. Managing the COMPUTING infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Social networking (also check the school Twitter policy)
- Video Conferencing

#### 5. Data security (GDPR Compliance)

- Management Information System access
- Data transfer

#### 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

#### **Appendices:**

1. Acceptable Use Agreement (Staff)
2. Staff Privacy Notice (Staff, Pupil, Parents, Lettings)
3. Acceptable Use Agreement including photo/video permission (Parents)

4. Protocol for responding to e-safety incidents and Data Breach incidents
5. Protocol for Safeguarding
6. Search and Confiscation guidance from DfE

## 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 Chalkhill Primary School with respect to the use of COMPUTING-based technologies.
  - Have robust processes in place to safeguard and to ensure the online safety of pupils, staff, volunteers and governors and comply with GDPR (General Data Protection Regulation).
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

#### Our approach to online safety is based on addressing the following categories of risk:

##### Content

- being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- exposure to inappropriate content, including online pornography,
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- Data breach
- content validation: how to check authenticity and accuracy of online content

## Contact

- being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- cyber-bullying in all forms
- identity theft and sharing passwords

## Conduct

- personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing/forwarding of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying;
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Messaging

## Commerce

- ☐ risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

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

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

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

### **Roles and Responsibilities**

Role	Key Responsibilities
The Headteacher	<ul style="list-style-type: none"><li>• Is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.</li><li>• To take overall responsibility for e-Safety provision</li><li>• To take overall responsibility for data and data security GDPR compliant</li><li>• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL</li><li>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant<ul style="list-style-type: none"><li>□ To be aware of procedures to be followed in the event of a serious e-safety incident.</li></ul></li><li>• To receive regular monitoring reports about E-Safety from Computing Coordinator</li><li>• To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures</li></ul>

<p>The Designated Safeguarding Lead/ E-Safety Lead</p>	<p>Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school</p> <p>Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents</p> <p>Managing all online safety issues and incidents in line with the school child protection policy</p> <p>Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy</p> <p>Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy</p> <p>Updating and delivering staff training on online safety</p> <p>Liaising with other agencies and/or external services if necessary</p> <p>Providing regular reports on online safety in school to the headteacher and/or governing board</p>
<p>The Governing Board</p>	<ul style="list-style-type: none"> <li>• The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.</li> <li>• The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety</li> </ul>

Role	Key Responsibilities
	<p>logs as provided by the designated safeguarding lead (DSL).</p> <p>All governors will:</p> <ul style="list-style-type: none"> <li>• Ensure that they have read and understand this policy</li> <li>• Agree and adhere to the terms on acceptable use of the school's ICT systems and the</li> <li>• Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable</li> </ul>

<p>ICT manager</p> <p>The school uses Village technicians for technical support</p>	<p>The ICT manager is responsible for:</p> <ul style="list-style-type: none"> <li>• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material</li> <li>• Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly</li> <li>• Conducting a full security check and monitoring the school's ICT systems on a weekly basis</li> <li>• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files</li> <li>• Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy</li> <li>• Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy</li> </ul>
<p>Data Protection Lead/ Data Protection Officer</p>	<ul style="list-style-type: none"> <li>• To take overall responsibility for data and data security</li> <li>• To ensure that all data held on pupils on the school office machines have appropriate access controls in place</li> </ul>
<p>LGfL Nominated contact(s)</p>	<p><input type="checkbox"/> To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts</p>
<p>Teachers</p>	<ul style="list-style-type: none"> <li>• To embed e-safety issues in all aspects of the curriculum and other school activities</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</li> <li>• 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</li> </ul>

Role	Key Responsibilities

All staff	<p>All staff, including contractors and agency staff, and volunteers are responsible for:</p> <p>Maintaining an understanding of this policy</p> <p>Implementing this policy consistently</p> <p>Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)</p> <p>Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy</p> <p>Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy</p> <p>Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'</p>
Pupils	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Pupil Acceptable Use Policy</li> <li>• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>• to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>• To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's ESafety Policy covers their actions out of school, if related to their membership of the school</li> <li>• To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home</li> <li>• To help the school in the creation/ review of e-safety policies</li> </ul>
Parent Support Advisor/E-Safety lead	<p><input type="checkbox"/> Educating Parents and raising awareness as instructed by Computing Coordinator</p>
Parents/carers	<ul style="list-style-type: none"> <li>• To support the school in promoting e-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</li> <li>• To read, understand and adhere to the school Twitter policy</li> <li>• To read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>• To access the school website /Twitter account accordance with the relevant school Acceptable Use Agreement.</li> <li>• To consult with the school if they have any concerns about their children's use of technology</li> </ul>

Role	Key Responsibilities
	<p>Parents are expected to:</p> <ul style="list-style-type: none"> <li>• Notify a member of staff or the headteacher of any concerns or queries regarding this policy</li> <li>• Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet</li> </ul> <p>Parents can seek further guidance on keeping children safe online from the following organisations and websites:</p> <ul style="list-style-type: none"> <li>• What are the issues? – <a href="#">UK Safer Internet Centre</a></li> <li>• Hot topics – <a href="#">Childnet International</a></li> <li>• Parent resource sheet – <a href="#">Childnet International</a></li> <li>• <a href="#">Healthy relationships – Disrespect Nobody</a></li> </ul>
Visitors and Members of the community	<ul style="list-style-type: none"> <li>• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school</li> <li>• To seek parental consent if the external party intends to use pupil photograph</li> <li>• Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.</li> </ul>

**Communication:**

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

- Policy to be posted on the school website/ staffroom.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

**Handling complaints:**

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by teacher / Phase Leader / e-Safety Coordinator / Headteacher;
  - informing parents or carers;



- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]; ○ referral to LA / Police.
- Our Head teacher acts as first point of contact for any e-safety complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our AntiBullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

### **Review and Monitoring**

The e-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school e- Safeguarding policy will be discussed in detail with all members of teaching staff.
- The school will monitor the impact of the policy using:

Logs of reported incidents

- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of ○ students/pupils ○ parents/carers ○ staff

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 2. Educating pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum: [National Curriculum computing programmes of study](#)

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

[Relationships education and health education](#) in primary schools

(Please note, our RSHE policy under consultation) In

**Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies Pupils in **Key Stage 2** will be taught to:

Use technology safely, respectfully and responsibly

Recognise acceptable and unacceptable behaviour

Identify a range of ways to report concerns about content and contact By

the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

**Staff and governor training** This school

- Ensures staff and governors have had GDPR training and know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes regular training available to staff on e-safety issues, GDPR and the school's esafety education program; Termly updates in staff meetings.
- 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 e-Safeguarding policy and the school's Acceptable Use Policies.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

### **Parent awareness and training**

Our school seek to provide information, awareness advice, guidance and training for parents/carers to ensure that principles of e-safety behaviour are made clear, through:

- Information leaflets; in school newsletters; on the school web site; Online Learning platforms

- demonstrations, workshops, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents. e.g. [swgfl.org.uk](http://swgfl.org.uk), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/), <http://www.childnet.com/parents-and-carers>
  - High Profile events/ campaigns such as *Safer Internet Day*, *Anti-bullying week*
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

### 3. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

#### Preventing and addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The Class teachers will discuss cyber-bullying with their class.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

## 4. Managing the Computing infrastructure

### □ Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search

engines where more open Internet searching is required; eg [yahoo for kids](#) or [ask for kids](#) , Google Safe Search , .....

- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that

Internet use is monitored;- Informs staff and

students that that they must report any failure of

the filtering systems directly to the [system

*administrator / teacher / person responsible for URL*

*filtering*]. Our system administrator(s) logs or

escalates as appropriate to the Technical service

provider or LGfL Helpdesk as necessary;

- Makes clear all users know and understand what the 'rules of appropriate use' are, GDPR compliance and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Computing devices provided by school to members of staff are regularly checked by the IT technicians.

#### □ **Network management (user access, backup)**

This school ○ Uses Technicians employed by Joskos till April 2022 then by The

Village ○ Uses individual, audited log-ins for all users - the London USO

system; ○ Uses guest accounts occasionally for external or short term

visitors for temporary access to appropriate services

- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

- Storage of all data within the school will conform to the GDPR requirements ○

Staff will only use encrypted USB sticks to hold any data about pupils *To ensure the network is used safely, this school:*

- Ensures staff read and sign that they have understood the school's E-safety Policy, Data Protection Policy, Data Retention Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. Guest users do not have access to our school's network;

- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with a year group network log-in username and password.
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform *and (for older pupils) their own school approved email account;*
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 5 mins and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 6 o'clock to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;  
e.g. teachers access report writing module; SEN coordinator - SEN data;

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:  
*e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAV3 system;*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;  
*e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children,*
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school computer systems regularly with regard to health and safety and security.

### **Passwords policy**

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



### **E-mail Chalkhill Primary school**

- All staff to adhere to school's Email protocol and email use policy
- Provides staff with an email account for their professional use, *London Staffmail (LGfL)* and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail address, for example [admin@chalkhill.brent.sch.uk](mailto:admin@chalkhill.brent.sch.uk) (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- 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.
- Any apps educational (Seesaw G--Suite for Education, Digimaps etc) and /or Classroom management (Class Dojo) used by school are GDPR compliant.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Any personal or business use for illegal, threatening, offensive, obscene, pornographic or libellous purposes by staff is strictly prohibited.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

### **Pupils:**

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.

- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments; ○ embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.

### **Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

**Staff:**

- Staff only use LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts is not permitted and may be blocked
- Never use personal email to transfer staff or pupil personal data. We use secure LGfL e-mail account.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted; ○ embedding adverts is not allowed;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
- A letter sent to anyone using the school letterhead must be approved by the head teacher.
- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school events on personal social networking sites such as Facebook. Twitter etc
- Staff must not use social networking sites within lesson times
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy

**School website**

- The Head of School takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- Admin staff: Ms Josna and Ms Ektaa, Ms Mallek and Deputy Headteacher.
- The school website complies with the [statutory DfE guidelines for publications](#);
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, [admin@chalkhill.brent.sch.uk](mailto:admin@chalkhill.brent.sch.uk) Home information or individual e-mail identities will not be published;
- 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;
- We do not use embedded geo-data in respect of stored images ○ We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

### **Social networking**

- 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.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils' parents/ carers or school staff
- Data about pupil/ staff or parents is not shared on social media
- 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 /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

### **Video Conferencing**

**This school** ○ Uses Google Meet, Zoom, Seesaw and ClassDojo for video conferencing activity;

### **CCTV**

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

**5. Data security: Management Information System access and Data transfer** (Also check our Data Protection Policy, Data Retention Policy and safeguarding policy)

### **Strategic and operational practices At**

this school:

- Staff to report any incidents where data may have been breached Data Protection Lead Ms Sheetal Shah and Irene Mallek and our Data Protection Officer **Deepti Bal.**
- 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 in the staff room and school office.
- We ensure All staff are DBS checked and records are held in one central record in the school office.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

- staff, ○
- governors, ○
- pupils ○
- parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

### **Technical Solutions**

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 5 mins idle time.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use RAv3 / VPN solution with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USO Auto Update, SIMS for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.

- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. <No back-up tapes leave the site on mobile devices.
- We use in house secure back-up for disaster recovery on our network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder.

## **6. Equipment and Digital Content**

School Mobile Devices such as Ipads, Chromebooks and laptops are used on the school network.

### **Staff using work devices out of school**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- The school will install anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Ms Hussian– the computing coordinator.

### **Personal mobile phones and mobile devices**

- Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils at time in the school including the school playground.
- Student mobile phones, MP3 players, iPads, smart watches which are brought into school must be turned off (not placed on silent) and handed in to the class teacher on

arrival at school. They must remain turned off and out of sight until the end of the day.

- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Staff mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the head teacher.
- Images and content recorded for twitter updates will be deleted from the school equipment once it is posted.

### ***Students' use of personal devices***

- The School strongly advises that student mobile phones/smart watches/tablets/MP3 players should not be brought into school. The school takes no responsibility for loss or damage of any personal devices brought to 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 student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Student mobile phones/smart watches/tablets/MP3 players should be handed to the class teacher upon arrival. Students found in possession of a mobile phone and or smart watch 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.
- 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.
- 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. However, in case if a student has sent an inappropriate message or photo to another student at any time and the matter is brought to the attention of the school then the device will be confiscated and returned at the end of the academic year. Parents/carers will be immediately informed.
- Students will be provided with school iPads/cameras/Chromebook/laptops to use in specific learning activities under the supervision of a member of staff. Such devices will be set up so that only those features required for the activity will be enabled.
- No students should use his or her mobile phone or personally-owned device in school. Any personal devices used in school by a pupil will be confiscated. Students should hand in their phones to the class teacher upon arriving to the classroom and collect it at the end of the day.

#### ***Staff use of personal devices***

- Staff handheld devices, including mobile phones and personal cameras must not be used during lesson times. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families outside of the setting in a professional capacity unless on a school trip.
- 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.
- The only circumstance in which a teacher can take a picture on the mobile phone is so that the image can be uploaded on the school's official twitter account. It should only be done with prior consent from the Head teacher. The image should be taken in



presence of teacher. The image/images should be deleted immediately once it is uploaded on the school's official twitter account.

- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should hide their caller identification. They can do so by inputting 141 to hide their own mobile number for confidentiality purposes.

### **Examining Electronic Devices**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or  Report it to the police\*

\* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

### **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 agreement form when their daughter / son joins the school; This will cover permission to use your child's photo/video on the school website/Twitter/ School learning apps such as G –suite/ Seesaw/ ClassDojo

- 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
- If specific pupil photos (not group 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 use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Photos/videos taken on school iPads are stored on the school network.
- Pupils are taught about how images can be manipulated in their e-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 identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

### **Asset disposal**

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the PRM Green Technologies website.

The school may also offer old IT equipment (that is deemed too slow and is no longer used by school such as an old laptop with less than I3 processor) to staff, once all the data and software including the firewall is erased by the IT technician.

### **How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour, E-safety and Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

### **E-safety Audit**

The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with LGfL guidance? Yes/No

Date of latest update (at least annual): \_\_\_\_\_

The Leadership team member responsible for e-safety is: \_\_\_\_\_

The governor responsible for e-Safety is: \_\_\_\_\_

The designated member of staff for child protection is: \_\_\_\_\_

The e-Safety Coordinator is: \_\_\_\_\_

The e-Safety Policy was approved by the Governors on \_\_\_\_\_

The policy is available for staff at: \_\_\_\_\_

The policy is available for parents/carers at: \_\_\_\_\_

### **Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)**

#### **ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS**

**Name of pupil:**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Ask a teacher or adult if I can do so before using them
- Only use websites/apps that a teacher or adult has told me or allowed me to use  Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## **Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)**

**ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS**

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it **I will not:**
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into school:**

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

**Signed (pupil):**

**Date:**

**Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

**Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and passwordprotected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

**Signed (staff member/governor/volunteer/visitor):**

**Date:**

#### **Appendix 4: online safety training needs – self audit for staff**

ONLINE SAFETY TRAINING NEEDS AUDIT

<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	