Online Safety policy

Approved by: Full GB
Approved Date: October 2019
Review Date: October 2020
# West Acton Primary School Online Safety Policy

## Contents

1. Overview ................................................................................................................................. 2  
2. Aims ............................................................................................................................................ 2  
3. Further help and support ......................................................................................................... 3  
4. Scope .......................................................................................................................................... 3  
5. Roles and Responsibilities ........................................................................................................ 3  
6. Curriculum and Education ....................................................................................................... 7  
7. Handling online safety concerns and incidents ......................................................................... 8  
8. Actions where there are concerns about a child ........................................................................ 9  
9. Sexting ...................................................................................................................................... 11  
10. Bullying ................................................................................................................................. 12  
11. Sexual Violence and Harrassment ......................................................................................... 12  
12. Misuse of School Technology (devices, systems, networks or platforms) ............................ 12  
13. Social Media Incidents .......................................................................................................... 12  
14. Data protection and data security .......................................................................................... 12  
15. Appropriate Filtering and Monitoring .................................................................................. 13  
16. Email ...................................................................................................................................... 13  
17. School Website ....................................................................................................................... 13  
18. Digital Images ....................................................................................................................... 13  
19. Staff, pupils' and parents online presence .............................................................................. 14  
20. Device Usage ............................................................................................................................ 15  
21. Searching and Confiscation ..................................................................................................... 15  

Appendix 1. Acceptable Use Agreement for Early Years .......................................................... 17  
Appendix 2. Acceptable Use Agreement for Key Stage 1 pupils ............................................ 18  
Appendix 3. Acceptable Use Agreement for Key Stage 2 pupils .............................................. 19  
Appendix 4. Acceptable Use Agreement for Parents ................................................................. 20  
Appendix 5. Acceptable Use Agreement for Staff .......................................................... 23
1. Overview

At West Acton Primary school, we recognise the importance of being digitally ‘connected’ to the wider world. Being part of the internet community provides limitless opportunities for learning. Unfortunately, this also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, grooming, cyber-bullying and identity theft. It is therefore the role of the school to ensure that such risks are minimised, and that children are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy on-line citizens.

Current and emerging technologies used in the school, and, more importantly in many cases, used outside of school by children include:

- The internet
- E-mail and instant messaging
- Chat rooms and social networking
- Blogs and Wikis
- Podcasting (audio sharing)
- Video sharing
- Music sharing (downloading)
- Gaming
- Mobile/Smart phones functionality including text, video, web, audio, music, global positioning (GPS)
- Other mobile devices with similar functionality (tablets, phones, laptops, gaming devices)

### Online Safety

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Safeguarding Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carole Ives</td>
<td>Deputy Head teacher</td>
<td>Designated Safeguarding Lead /Online Safety Lead (DSL)</td>
</tr>
<tr>
<td>Karen Kondo</td>
<td>Head teacher</td>
<td>Designated Deputy Safeguarding Lead (DDSL)</td>
</tr>
<tr>
<td>Rickiesha Williams</td>
<td>Pupil and Family Worker</td>
<td>Designated Deputy Safeguarding Lead (DDSL)</td>
</tr>
<tr>
<td>David Donnarumma</td>
<td>Chair of Governors</td>
<td>Safeguarding Governor</td>
</tr>
<tr>
<td>Omar Beno</td>
<td>Governor</td>
<td>Deputy Safeguarding Governor</td>
</tr>
</tbody>
</table>

2. Aims

This policy aims to:

- Set out expectations for all West Acton Primary School community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
• Facilitate the safe, responsible and respectful use of technology to support teaching &
learning, increase attainment and prepare children and young people for the risks and
opportunities of today’s and tomorrow’s digital world, to survive and thrive online
• Help school staff working with children to understand their roles and responsibilities to
work safely and responsibly with technology and the online world:
  • for the protection and benefit of the children and young people in their care, and
  • for their own protection, minimising misplaced or malicious allegations and to
    better understand their own standards and practice
  • for the benefit of the school, supporting the school ethos, aims and objectives, and
    protecting the reputation of the school and profession
• Establish clear structures by which online misdemeanours will be treated, and procedures
to follow where there are doubts or concerns (with reference to other school policies such
as Behaviour Policy or Anti-Bullying Policy)

3. Further help and support

Online safety incidents are reported as a safeguarding concern in line with our Safeguarding
Policy. The Designated Safeguarding Lead (DSL) will be told about the incident in person if it is
urgent or through our reporting system ‘MyConcern’. Where appropriate the concern will be
referred to the local authority.

Our website page for online safety has links to useful websites for parents and staff including:

Beyond this, reporting.lgfl.net has a list of links to external support and helplines for both pupils
and staff, including the Professionals’ Online-Safety Helpline from the UK Safer Internet Centre
and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud
which will be shared with parents, and anonymous support for children and young people.

4. Scope

This policy applies to all members of the West Acton Primary School community (including staff,
governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users)
who have access to our digital technology, networks and systems, whether on-site or remotely, and
at any time.

5. Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline,
to use technology for teaching and learning and to prepare for life after school, and to immediately
report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation
of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

**Head teacher/Deputy Designated Safeguarding Lead**

**Key Responsibilities**
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding and ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Ensure that policies and procedures are understood and followed by all staff and ensure that all staff receive suitable training to carry out their safeguarding and online safety roles
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Ensure governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety
- Ensure the school website meets statutory DfE requirements (see appendices for website audit document)

**Designated Safeguarding Lead/ Online Safety Lead (DSL)**

**Key responsibilities**
- Act as a named point of contact on all online safeguarding issues and to liaise with other members of staff or other agencies as appropriate
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident on My Concern
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response, policies and procedures
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
  - all staff must read KCSIE Part 1 and all those working with children Annex A
  - it would also be advisable for all staff to be aware of Annex C (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation
  - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

**Governing Body**

**Key responsibilities**
- Read, understand, contribute to and help promote the school’s online safety policy and guidance
• Develop an overview of the benefits and risks of the internet and common technologies used by pupils
• Understand how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
• Develop an overview of how the school computing infrastructure provided safe access to the internet (https://www.lgfl.net/online-safety/)
• Have regular strategic reviews with the Online Safety Lead/OSL and incorporate online safety into standing discussions at governor meetings

All Staff
Key Responsibilities
• Understand that online safety is a core part of safeguarding; as such it is part of everyone’s job – never think that someone else will pick it up
• Know who the Designated Safeguarding Lead (DSL)/ Online Safety Lead (OSL) is
• Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
• Read and follow this policy in conjunction with the school’s main safeguarding policy
• Record online-safety incidents in the same way as any safeguarding incident on MyConcern and report in accordance with school procedures.
• Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
• Sign and follow the staff acceptable use policy and code of conduct
• Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum
• Whenever overseeing the use of technology in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites
• To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
• Take a zero-tolerance approach to bullying and low-level sexual harassment
• Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

Network Manager – TRUSOL (External Provider)
Key responsibilities:
• As listed in the ‘all staff’ section, plus:
• 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
• Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL TRUSTnet nominated contact to ensure that school systems and networks reflect school policy
• Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team
• Maintain up-to-date documentation of the school’s online security and technical procedures
• To report online-safety related issues that come to their attention in line with school policy
• Manage the school’s systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

• Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

**Data Protection Officer – Head teacher/Judicium**

Key responsibilities:

• Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (April 2018), especially this quote from the latter document:

> ‘GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.’

• The same document states that the retention schedule for safeguarding records may be required to be set as ‘Very long term need (until pupil is aged 25 or older)’

• Work with the DSL, Head teacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.

• Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

**Pupils**

Key responsibilities:

• Read, understand, sign and adhere to the pupil acceptable use policy

• Understand the importance of reporting abuse, misuse or access to inappropriate materials

• Understand how to report abuse by using ‘The Space’, talking to Year 5 and Year 6 Cybermentors, talking to their parents or an adult at school

• 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 and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school’s acceptable use policies cover actions out of school, including on social media

• Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

**Parents/Carers**

West Acton Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet

Key responsibilities:

• Read, sign and promote the school’s parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it

• Consult with the school if they have any concerns about their children’s use of technology
• Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other’s images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

External Groups including Parent Associations
Key responsibilities:
• Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
• Support the school in promoting online safety and data protection
• Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other’s images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Volunteers and Contractors
Key responsibilities:
• Read, understand, sign and adhere to an acceptable use policy (AUP)
• Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
• Maintain an awareness of current online safety issues and guidance
• Model safe, responsible and professional behaviours in their own use of technology

6. Curriculum and Education
It is important to teach pupils about the underpinning knowledge and behaviours that can help them navigate the online world safely and confidently regardless of the device, platform or app. As a school we are very aware of the risks that exist online so teaching and support is tailored to the specific needs of our pupils.

Underpinning knowledge and behaviours include:
• How to evaluate what they see online
• How to recognise techniques used for persuasion
• Online behaviour
• How to identify online risks
• How and when to seek support

New government guidance Teaching-online-safety-in-schools 2019 outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. We have embedded online safety across the curriculum throughout the whole school in order to raise awareness and promote safe and responsible internet use amongst pupils by:
• Through Relationships Education and Health Education pupils are taught about what positive, healthy and respectful online relationships look like, the effects of their actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects online safety and appropriate behaviour are taught in an age appropriate way that is relevant to pupils lives
• The computing curriculum (Purple Mash) covers the principles of internet safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Other curriculum subjects also include content relevant to teaching pupils how to use the internet safely. For example citizenship education covers media literacy – distinguishing fact from opinion as well as exploring freedom of speech and the role of and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights and responsibilities.
- We ask all pupils to sign an acceptable use policy (AUP). This outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
- We support pupils to read and understand the AUP in a way which suits their age and ability by displaying acceptable use posters in all rooms with internet access, informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation, rewarding positive use of technology by pupils and seeking pupil voice when developing safer internet practice.
- Our Year 5 and Year 6 Cyber mentors support pupils with learning about safer internet use and are also to available to answer any questions or discuss any concerns at break times.
- Inviting external visitors where appropriate to compliment and support the schools internal online safety education approaches.

Vulnerable pupils (including those in EYFS and the ARP)
West Acton Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with special educational needs or disabilities, children with mental health needs, children with English as a second language (EAL) and children experiencing trauma or loss. We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils seeking external guidance as needed.

The following resources are used to consider how best to support our most vulnerable pupils stay safe online:
- Vulnerable Children in a Digital World
- Children's online activities, risks and safety
- Star SEN toolkit - childnet

Whenever overseeing the use of technology in school or setting as homework tasks, all staff encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. Regularly updated theme-based materials and signposting for teachers and parents are available on Lgfl online safety resources.

At West Acton Primary School, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum. Reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to embed the key areas of Self-image and Identity,
Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership into the curriculum.

7. Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding as well as being a curriculum strand. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the OSL/DSL to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online safety are also detailed in the following policies (primarily in the first key document):

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Anti-Radicalisation Policy
- Data Protection Policy

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school’s escalation processes.

Any suspected online risk or infringement must be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline posters.lgfl.net and reporting.lgfl.net.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre’s Professionals’ Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting; see section below).

8. Actions where there are concerns about a child

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2019 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.
(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child’s life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child’s welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).
9. Sexting
All schools should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as ‘youth produced sexual imagery’) in schools. Sexting in Schools and Colleges (Responding to incidents and safeguarding young people). NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.
There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.
The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.
It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.
The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net
10. Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. It is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

11. Sexual Violence and Harassment

In 2018 new Department for Education guidance was issued on sexual violence and harassment, as a new section within Keeping Children Safe in Education and also as a document in its own right. Sexual violence and harassment between children in schools and colleges. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as ‘low level’ are treated seriously and not allowed to perpetuate.

12. Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/, devices and other technology. Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

13. Social Media Incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the West Acton Primary School community. These are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school behaviour policy (for pupils) or Staff code of conduct (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, West Acton Primary School will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals’ Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

14. Data protection and data security

We will ensure personal data is recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.
Staff will not remove personal or sensitive data from the school premises without permission of the leadership team. Any data which it is impractical to ensure is kept in school will be kept secure, by use of school laptops which are password protected or on an encrypted USB Flash drive.

15. Appropriate Filtering and Monitoring
Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material but at the same time be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, LGfL TRUSTnet provides the internet connection. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

If users discover a website with inappropriate content, this is reported to the DSL/Internet Safety Lead.

16. Email
Staff use the LGFL approved email account allocated to them by the school, and are aware that their use of the school email system will be monitored and checked. Staff or pupil personal data should never be sent/shared/stored on email. If staff need to share data with external agencies, Egress must be used. Pupils are not allocated an individual email account.
Communication between staff and the local community should be professional and related to school matters only. Any inappropriate use of the school email system, or the receipt of any inappropriate messages by a user is reported to a member of the senior leadership team.

17. School Website
The school website is part of our online presence and hence all content and images are carefully monitored by the Head teacher. The content of the website is composed in such a way that individual pupils cannot be clearly identified.
Staff and pupils should not post school-related content on any external website without seeking permission first.
A generic contact email (admin@west-acton.ealing.sch.uk) is used for all enquiries received through the school website.

18. Digital Images
When a pupil/student joins the school, parents/carers are asked if they give consent for their child’s image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:
- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media
Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them). All staff are governed by their contract of employment and the school’s Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At West Acton Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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.

19. Staff, pupils’ and parents online presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government’s Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope
with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don’t need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night’s sleep and productive teaching and learning at school the next day).

Pupils/students are not allowed* to be ‘friends’ with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from ‘following’ staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head teacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head teacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

20. Device Usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal Devices BYO

Pupils/students in Year 5 and Year 6 are allowed to bring mobile phones into school however these must be handed in to the school office on arrival. They are then collected at the end of the day.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours.

Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head teacher should be sought (the Head teacher may choose to delegate this) and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to parentfilming.lgfl.net for further guidance.
21. Searching and Confiscation
In line with the DfE guidance ‘Searching, screening and confiscation: advice for schools’, the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.
Appendix 1. Acceptable use Agreement for Early Years Pupils

Acceptable Use Agreement
(For EYFS)

- I ask before I use a tablet, computer or camera.
- I tap or click on things I have been shown.
- I check if I can tap/click on things I haven’t seen before.
- I tell a grown-up if something upsets me.

My Name: [Type name here]
Class: [Type class here]
Parent/Carer Signed: [Type date here]
Today's Date: [Type date here]

www.2simple.com
Leading Standards Through Creativity

Contact us:
Tel: 0298 103 1781
Email: support@2simple.com
Appendix 2. Acceptable use Agreement for Key Stage 1 pupils

Acceptable Use Agreement

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don’t follow it.

My Name: Type name here  Class: Type class here

Parent/Carer Signed:  Today’s Date: Type date here
Appendix 3. Acceptable Use Agreement for Key Stage 2 Pupils

Acceptable Use Agreement

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others’ personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.

- I will respect computing equipment and will immediately notify an adult if I notice something isn’t working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn’t approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.
  T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?

I understand this agreement and know the consequences if I don’t follow it.

My Name: Type name here
Class: Type class here
Parent/Carer Signed: Type date here
Today’s Date: Type date here
Appendix 4: Acceptable Use Agreement Parent/Carer

Acceptable Use Agreement

(For Parents/Carers)

**Background and purpose**

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This Parent/Carer Acceptable Use Agreement is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child’s online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

**Parents/Carers**

We would ask parents and carers to support us by:

- Sharing good online behaviours with your child.
- Emphasising the importance of the Acceptable Use Statements/School’s rules your child has agreed to.
- Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- Explaining how to keep an appropriate digital footprint.
- Discussing what is and isn’t appropriate to share online.
- Emphasising never to meet anyone online nor trust that everyone has good intentions.
- Reporting any concerns you have whether home or school based.
- Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend’s home.
- Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

**Permission Access**

By signing below, you agree to allowing your child access to the school’s internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school’s Acceptable Use Agreement for pupils.

**Your Child's Name:**

Type name here

**Class:**

Type class here

**Parent’s/Carer’s Signature:**

Date:

Type date here

*The school aims to comply with GDPR regulations at all times and as such follows strict protocol about how we use personal data and keep it safe, including the information on this form. It is important that you refer to the school’s data protection policy or contact the school if you have any questions about data.*
Online Safety Tips

- Explain how to keep an appropriate digital footprint
- Emphasise never to meet anyone online or trust strangers
- Avoid posting or replying to any comments about the school on social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance
- Highlight the importance of accessing age-appropriate content and sites, along with the dangers of social media
- Report any concerns you have whether home or school based
- Share good online behaviours with your child
- Stress the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact
- Emphasise the importance of the Acceptable Use statements/School’s rules your child has agreed to
- Discuss what is and isn’t appropriate to share online
- Draw up an agreement of online safety rules on the next page that are applicable even when your child is at a friend’s house
Our Home Online Safety Rules

1. Enter rule here
2. Enter rule here
3. Enter rule here
4. Enter rule here
5. Enter rule here
6. Enter rule here
7. Enter rule here
8. Enter rule here
9. Enter rule here
10. Enter rule here
Appendix 5: Acceptable Use Agreement Staff

Acceptable Use Agreement

(Staff)

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children’s learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

The school’s internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school’s systems and acknowledge that you agree to all the statements below. Additionally, you have read and understood school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school’s policies.
- I understand my use of the school’s ICT systems/networks and internet are monitored.
- I understand that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school’s data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school’s social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others’ behaviours/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person.
- Any school trips/ outings or activities that require a mobile phone/camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point will I use my own devices for capturing images/video or making contact with parents/carers.

Staff Name: [Type name here]  Signature:  Date: