Hotham Primary School
Online Safety Policy

Autumn 2023

Ownership and Consultation	
Document author (name and role)	Rebecca Oddy, Assistant Headteacher (DSL)
Consultation (role)	The Key Model Policy, ELT, Governors
Approval	Full Governing Body

Version Control	
Approval date	September 2023
Implementation date	September 2023
Review date	September 2024

Related documentation/resources	Child Protection and Safeguarding policy; Behaviour Policy; Anti-Bullying Policy; Staff Code of Conduct; Staff Handbook; Staff Disciplinary Procedures; Data Protection Policy and Privacy Notices; Complaints Policy; RHE policy

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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

The four key categories of risk

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
- **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
- **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 of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. 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

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 cyber-bullying 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Jane Mitchell.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix E)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- 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

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL, deputy DSL and other staff members trained to DSL level are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The School Business Manager (SBM)

The SBM is responsible for:

- 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis with support from Wandsworth IT services
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Liaise with the Headteacher to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix E), and ensuring that pupils follow the school's terms on acceptable use (appendices A, B, C and H)
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices A,, B, C and H)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix E).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

The text below is taken from the 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
- Relationships and sex education and health education in secondary schools

In **Early Years Foundation Stage (EYFS**) children are taught to:

- Use technology safely and respectfully, keeping personal information private
- Seek help from an appropriate adult if something appears to have gone wrong or if they see something that they don't think is right

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
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

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.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

6. Cyber-bullying

6.1 Definition

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. (See also the school behaviour policy.)

6.2 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.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 13 for more detail).

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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- School behaviour policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Hotham Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Hotham Primary School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. 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 A, B, C and H). 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. The Wifi password will not be shared with visitors unless it is applicable whilst visiting Hotham.

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 A, B and C. Appendix H also includes information about acceptable use of Google Classroom for pupils.

8. Pupils using mobile devices in school

Pupils in Y5 and Y6 only may bring mobile devices into school, but they must be handed in to their class teacher at the start of the school day and they will be kept securely in a locked cupboard. They are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school
- Break times

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices A, B, C and H).

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.

9. Staff using work devices outside 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)
- Ensuring any USB containing school data is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing 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 E.

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 the SBM.

10. Pupils using school devices outside school

All pupils, with the support of their parent/carer 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
- Keeping operating systems up to date – always install the latest updates

Pupils, with the support of their parent/carer must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix A, B, C and H.

School devices must be used solely for school activities.

If pupils or their parent/carer have any concerns over the security of their device, they must seek advice from the SBM.

11. Online Live Teaching

In the situation where we are providing online live teaching we will follow school policies. For example:

- Live teaching lessons will be password protected and recorded
- Passwords and links will be shared within Google Classroom or via emails to parents/carers
- Where possible there will always be two members of staff in any online live teaching where children are engaging in the lesson (either via camera or typed comments)

Any safeguarding concerns should be raised with a DSL in the usual manner. For parents email DSL using info@hotham.wandsworth.sch.uk or if urgent ring the school.

12. 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 behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. All incidents of pupil misuse will be logged on CPOMS, tagged appropriately.

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 disciplinary procedures. 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.

13. Training

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 and Deputy 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.

14. Monitoring arrangements

All staff must log behaviour and safeguarding issues related to online safety on CPOMS. The DSL and other designated members of staff will monitor behaviour and safeguarding issues related to online safety and the respective follow up actions.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available here) 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.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy (which includes our policy on Bullying)
- Staff Code of Conduct / Staff Handbook / Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Remote Learning Policy

Appendix A – EYFS Student Acceptable Use Agreement

Think before you click	
S	I will only use the Internet and email with an adult.
A	I will only click on icons and links when I know they are safe.
F	I will only send friendly and polite messages.
E	If I see something I don't like on a screen, I will always tell an adult.

My Name: ____

My Signature: ____

Appendix B – KS1 Student Acceptable Use Agreement

A London Grid for Learning / TRUSTnet brand

Key Stage 1: Pupil Acceptable Use Agreement

This is how I keep **SAFE online**: ✓

1. I only use the devices I'm **ALLOWED** to □
2. I **CHECK** before I use new sites, games or apps □
3. I **ASK** for help if I'm stuck □
4. I **THINK** before I click □
5. I **KNOW** people online aren't always who they say □
6. I don't keep **SECRETS** just because someone asks me to □
7. I don't change **CLOTHES** in front of a camera □
8. I am **RESPONSIBLE** so never share private information □
9. I am **KIND** and polite to everyone □
10. I **TELL** a trusted adult if I'm worried, scared or just not sure □

My trusted adults are ______________________ at school

______________________ at home and ______________________

My name is _________________________

Appendix C – KS2 Student Acceptable Use Agreement

A London Grid for Learning / TRUSTnet brand

Key Stage 2: Pupil Acceptable Use Agreement

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

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, games and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

- ***I am a responsible user of a mobile phone*** – If I am allowed to bring my mobile phone to school, I turn it off and leave it in the school office. I will also leave my mobile phone at school or at home if I am going on a school trip.
- ***I am considerate user of school iPads and computers*** – I do not login as other users and I do not edit or delete other children's work.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: ______________________________ Date: ______________

Appendix D – Parents online safety and photos agreement

Parents are asked to answer the following questions on the school data collection form when their child starts at Hotham Primary School:

- **E-Safety -** As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL e-mail or School Gmail and other ICT facilities at school. I know that my daughter or son will sign an Acceptable Use Agreement form and that they have rules for responsible ICT use. I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.I understand that if they have concerns about their e-safety or e-behaviour that they will contact me.I understand that the school can confiscate personal equipment to ensure the safety of all children at Hotham Primary School.I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

- **Social Media** - Hotham uses social media to celebrate things happening in School (we never use children's surnames). Some of the social media we use include a weekly newsletter which is emailed to parents, our school website and teachers Twitter accounts. Are you happy for your child's photo to be included?

- **Google classroom** - we share photos and videos of the children via our google classroom. This can only be accessed by Hotham families with a password. Can a photo or video of your child be shared this way?

- Occasionally DBS checked third parties would like to use photos of our pupils. These would be authors visiting Hotham, sports coaches working with the pupils, Wandsworth Council's school brochure or people running workshops with the children. Can they photograph your child as part of their work? No names will be used on these publications.

Appendix E – Staff, Volunteers, Governors and Contractors Acceptable Use Agreement

A London Grid for Learning / TRUSTnet brand

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors

Covers use of all digital technologies while in school: i.e. **email, internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school or school umbrella body (Local Authority, Academy, Free School Trust, etc).**

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

Hotham Primary School regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *Hotham email / LGfL StaffMail*
- I will only use the approved method/s of communicating with pupils or parents/carers: [*Hotham email / LGfL StaffMail]* and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact Dafinka Dimitrova.

- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will not use them in classrooms and only use them in the staff room during the school day.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer, laptop, iPad or camera loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption (including USBs) and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I am aware that under the provisions of the UK GDPR (UK General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead [Sarah Martin].
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- *Staff that have a teaching role only:* I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.
- I understand that storage space on the network is limited. I will ensure that old unused files are removed from the network at the end of each academic year. If I am unsure of what can be safely deleted I should ask the ICT technician for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician and ELT
- I will only save things onto school computers that are needed and appropriate for school (this includes music and photos).

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors

User Signature

I agree to abide by all the points above.

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

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

I understand that all Internet usage / and network usage can be logged and this information could be made available to my line manager on request.

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

Signature Date

Full Name (printed)

Job title / Role

Authorised Signature (Head Teacher / Deputy)

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

Signature Date

Full Name (printed)

Appendix F – Student user agreement infringements

Consequences for inappropriate use of internet

Category A infringements:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons

e.g. to send texts to friends

- Use of unauthorised instant messaging / social networking sites / online games

Sanctions: Class teacher to deal with and inform the parent of child involved.

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms / social networking sites / online games
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Sanctions: Phase leader to deal with and inform the parent of child involved.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or instant message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Sanctions: Referred to SLT and Safeguarding Lead. Inform the child's parents. Further sanctions in line with the school behaviour policy. Further safeguarding actions in line with the safeguarding policy

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform ICT technician and LGfL

Category D infringements

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of UK GDPR
- Bringing the school name into disrepute

Sanctions – Referred to SLT/|ELT and Safeguarding Lead / Contact with parents / serious sanction in line with the behaviour policy/ removal of equipment.

Appendix G – Glossary/Key terms

Assessing risks

- Managing Emerging Technologies: Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- No children will be allowed unsupervised access to the internet at Hotham Primary School.
- The school will audit ICT provision to establish if the online safety Policy is adequate and that its implementation is effective.

Cyber Bullying

Cyber bullying is when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else. The school will help prepare pupils for the hazards of using technology while promoting learning and social opportunities. Cyber bullying is a form of bullying but because it happens online or on mobile phones it can happen 24 hours a day, seven days a week.
Being cyber bullied can be very painful for those who are the targets and so pupils need to be taught about how to deal with it. The school will help prepare pupils for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media pupils can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Any issues of Cyber Bullying will be dealt with in line with the Anti-Bullying Policy.

Digital Video and Images

- Video conferencing is allowed at school as long as it follows LGfL guidance
- Teachers cannot use their own personal cameras at school, the school will provide digital cameras or iPads for school use.
- Images of pupils can be included in work around the school unless parents have indicated otherwise.
- Images of pupils cannot be used on the school website without the permission of parents/carers.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- All staff must use the Hotham approved staff e-mail (or LGfL email) for all school related e-mails

Online safety disclosures

- Disclosures regarding electronic devices or the online environment will be dealt with in the same way as explained in the Safeguarding policy.
- Wandsworth's Safeguarding Children Board recommends in its Online safety policy that every school has a designated Online safety lead officer (ESLO), Hotham’s will be the same as our Designated Safeguarding Lead (DSL).

Filtering

- We will work in partnership with the Local Authority, Becta, LGfL and the Internet Service Provider to ensure filtering systems are as effective as possible.

Handling online safety complaints and concerns

- All complaints will follow the school complaints policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to a member of the senior leadership team.

Internet use

- Access to the Internet will be under adult supervision to access specific, approved on-line materials.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Mobile phones

Pupils:

- Pupils are not allowed to use mobile phones at school, they need to be handed into a member of staff at the beginning of school of the day and collected at the end of school day.

Teachers:

- Teachers are not allowed to use mobile phones in lessons (including cameras), during the school day they should only be used in the staff room.
- Cameras cannot be used to take or store photos of children.
- Mobile phone calls are not allowed to be answered during lesson times, and they should be made in the staff room or outside of the school perimeter.
- Mobile phones are allowed on school trips.
- Mobile phones should have a passcode enabled to prevent any personal information being obtained by pupils.

Prevent Duty and Online safety

- All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.
- In line with our commitment to minimise the risk of pupils being radicalised, pupils' use of school computers is monitored and pupils found searching websites or using criteria that would suggest an interest in terrorism/radicalisation are immediately reported to the safeguarding team via a cause for concern form. The matter will then follow the procedures set out in the safeguarding policy.
- Please refer to the DfE Keeping children safe in education and Prevent document as well as our Child Protection Policy for further information.

School network safety measures

- The school maintains broadband connectivity through the LGfL
- Virus protection is installed and updated regularly.
- To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into files through Internet use, staff and pupils are not able to download executable files and software. Unfortunately, there is the potential for inappropriate material to get through any filtering system.

School staff

All staff are responsible for promoting and supporting safe behaviours in classrooms and the wider school by following school online safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials. All staff should be familiar with Hotham’s online safety Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services including social networking;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as digital cameras and camcorders;
- Publication of pupil information/photographs and use of the school website;
- Cyber Bullying procedures;
- Their role in providing online safety education for pupils

All staff will be given the online safety Policy at the beginning of each school year and its importance will be explained. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. It will be made clear that discretion and professional conduct is essential.

Training will be provided to all staff at the same time as training in child protection as well as in some Computing/ICT CPD.

Sexting/Youth Produced Sexual Imagery

Sexting is when someone shares sexual, naked or semi-naked images of themselves or others, or sends sexually explicit messages. They can be sent using mobiles, tablets, smartphones, laptops – any device that allows you to share media and messages.

Sexting can be seen as harmless by young people but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

- Take an explicit photo or video of themselves or a friend.
- Share an explicit image or video of a child, even if it is shared between children of the same age.
- Possess, download or store an explicit or video of a child, even if the child gave their permission for it to be created.

In the most recent guidance produced by the UK Council for Child Internet Safety, Sexting in Schools and Colleges Resource Pack, sexting is referred to as “youth produced sexual imagery”, although KCSIE still refers to “sexting”. Incidents of “sexting” will be investigated and dealt with in line with the safeguarding policy.

Social Networking

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social media space.
- Pupils will learn about how to make their profiles private and sensibly use Social networks.
- Pupils will be advised about security and taught about secure passwords (and not sharing them) as well as blocking unwanted communications.
- Pupils will also learn about report features on social networking sites to be used if they have any problems.

Appendix H – Google classroom guide for students (with expectations)

How to use Google Classroom for Hotham Students

Hello Hotham students! Welcome to Google Classroom.
Here are some instructions about how to use it.
If you can't read this, your parent or someone at home will need to read it to you.

Important information:

- **E-safety**
  - Do not share your password with other students.
  - If you feel unsafe, tell someone! Your parents need to email info@hotham.wandsworth.sch.uk with the email subject **Concerns in Google classroom**
  - Don't edit other people's work

- **How to behave in Google Classroom**
  - Remember that everyone can see what you have written (teachers included).
  - BE KIND and don't fill the stream with random or silly comments. If you wouldn't say it to the person or in front of your teacher, don't say it on Google classroom.
  - If you make a mistake please edit or delete your post.
  - Do not post links or YouTube videos into conversations without checking with your parents. Any inappropriate videos or links will be considered unwanted behaviour.

- **Unwanted behaviour**
  - If you write something silly, unkind or inappropriate, teachers will delete comments and a warning will be given to you in the stream.
  - If you continue, you will receive a second warning in the stream.
  - If you continue after this, your account will be muted, you will receive a third warning and your parents will be informed.
  - After you are unmuted, if you continue with any unwanted behaviour, we will consider what happens next and you may be removed from Google classroom!

Using Google Classroom

You will need to use the two main tabs 'Stream' and 'Classwork':

Stream (when it is turned on):

- Where **you** can write to your classmates and teacher and ask questions. (If your parents have a question, they can email info@hotham.wandsworth.sch.uk)

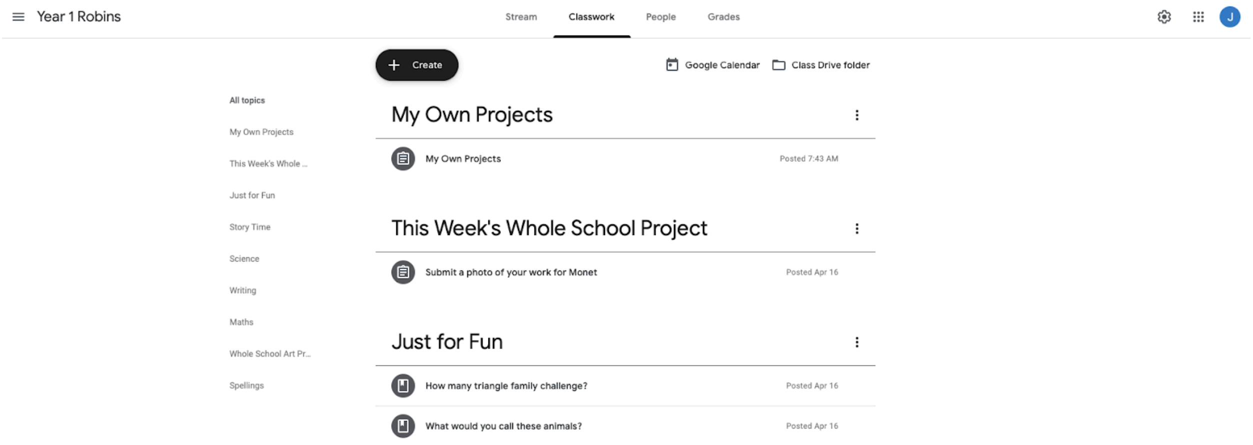
- You can share photos or anything you have been learning about.

- Remember our Hotham values: **Respect, Responsibility and Resolve** and things like full stops and capital letters.

- It tells you when things have been posted.

- Adults from school might say hello.

Classwork:



My Own Projects

My Own Projects — Posted 7:43 AM

This Week's Whole School Project

Submit a photo of your work for Monet — Posted Apr 16

Just for Fun

How many triangle family challenge? — Posted Apr 16

What would you call these animals? — Posted Apr 16

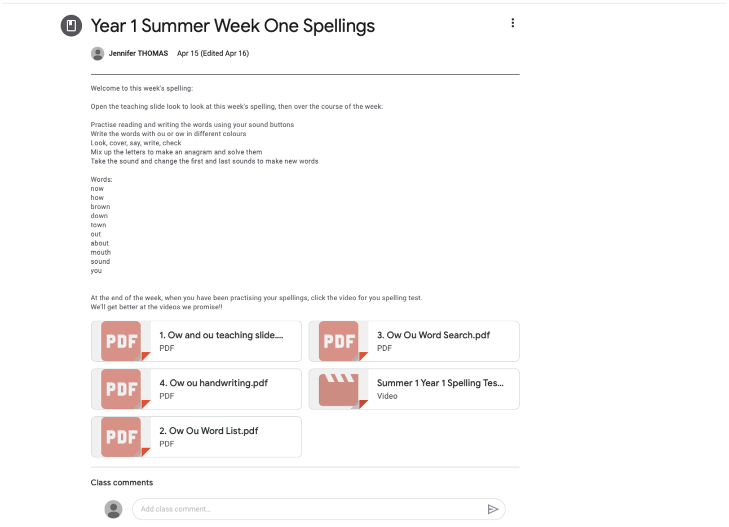
- Stores your work.

- Organised into topics/subject areas.

- Where you TURN IN your work.

<u>Reading and learning the resources</u>

1. **Click on the subject area e.g. Spellings and then on an assignment/material.**
2. **Read the welcome text that drops down (and click on the instructions pdf where they are available) and then click on each file to open.**



Year 1 Summer Week One Spellings

Jennifer THOMAS Apr 15 (Edited Apr 16)

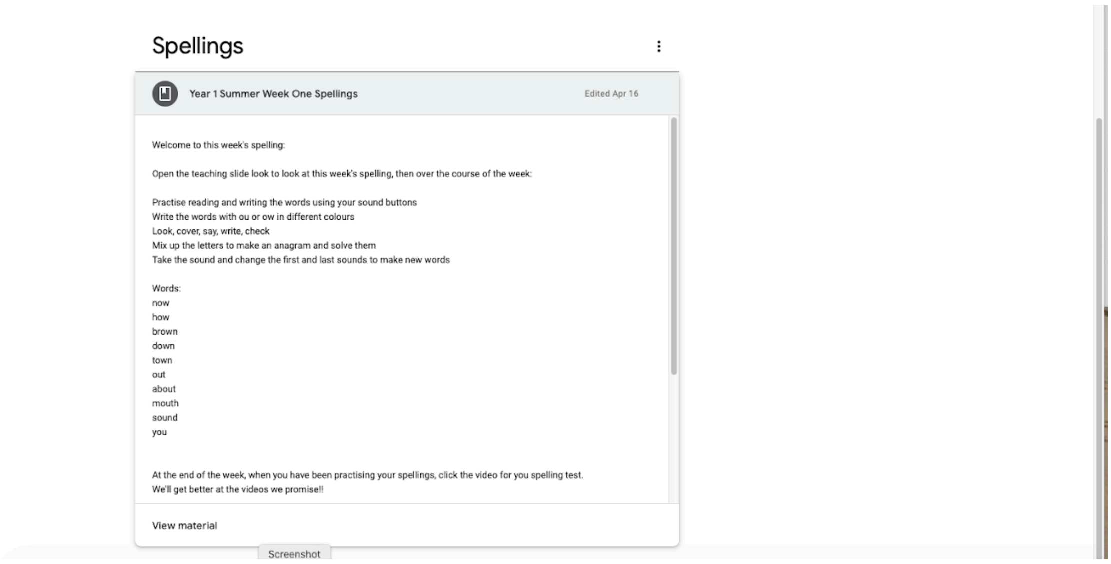
Welcome to this week's spelling:

Open the teaching slide look to look at this week's spelling, then over the course of the week:

Practise reading and writing the words using your sound buttons
Write the words with ou or ow in different colours
Look, cover, say, write, check
Mix up the letters to make an anagram and solve them
Take the sound and change the first and last sounds to make new words

Words:
now
how
brown
down
town
out
about
mouth
sound
you

At the end of the week, when you have been practising your spellings, click the video for you spelling test.
We'll get better at the videos we promise!!



Spellings

Year 1 Summer Week One Spellings

Edited Apr 16

Welcome to this week's spelling:

Open the teaching slide look to look at this week's spelling, then over the course of the week:

Practise reading and writing the words using your sound buttons
Write the words with ou or ow in different colours
Look, cover, say, write, check
Mix up the letters to make an anagram and solve them
Take the sound and change the first and last sounds to make new words

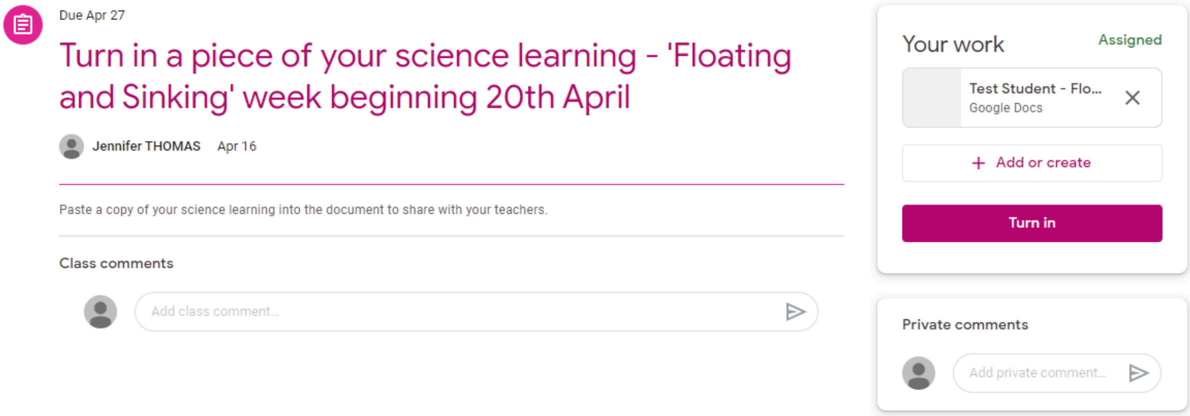
Words:
now
how
brown
down
town
out
about
mouth
sound
you

At the end of the week, when you have been practising your spellings, click the video for you spelling test.
We'll get better at the videos we promise!!

- Files will be often numbered so they are easier to find, so all the files for activity 1 have 1 at the front and so on…

- Some tasks will have mild, spicy or hot choices that you can choose from. Look out for your class/age to see which one to use as a starting point.

Turning in an assignment



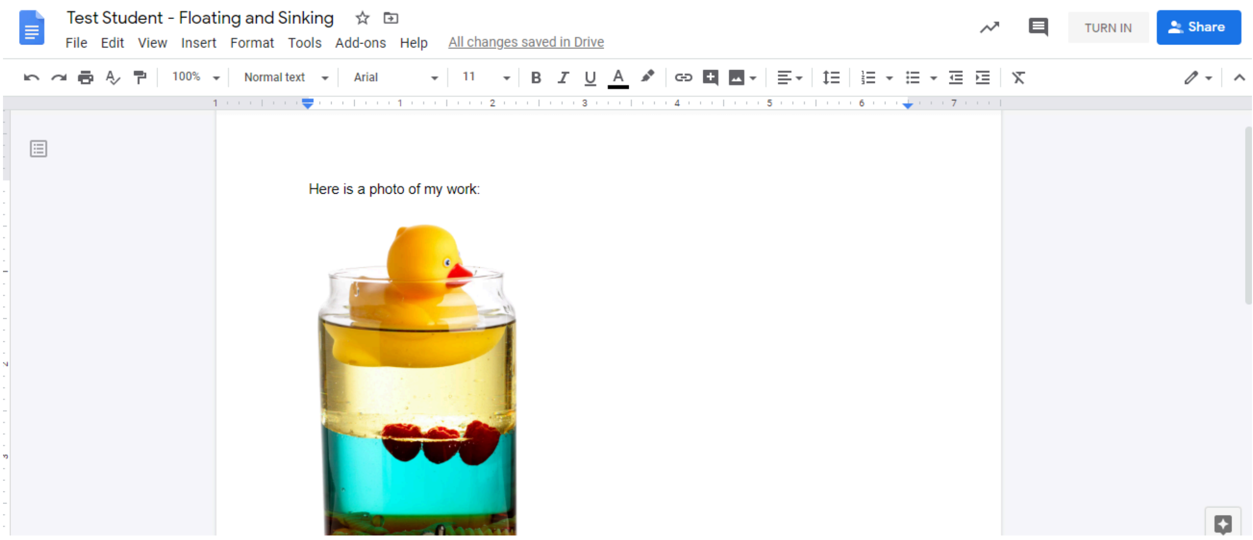
Due Apr 27

Turn in a piece of your science learning - 'Floating and Sinking' week beginning 20th April

Jennifer THOMAS Apr 16

Paste a copy of your science learning into the document to share with your teachers.

1. Within the assignment click on the document in **'Your work'**
2. This opens a page where you can type or add photos of your work. You can use '**insert'** and then upload an image from your device or from Google drive. You can also **paste** images. If you have done a piece of writing, we don't expect you to type it out. A photo is fine!


Test Student - Floating and Sinking
File Edit View Insert Format Tools Add-ons Help
All changes saved in Drive
TURN IN
Share
100%
Normal text
Arial
11

Here is a photo of my work:

0. Once you have finished, click **TURN IN** and the work is sent to your teacher. If you want to change anything after you have pressed this, you can open and edit the document after. Then click **TURN IN** and the edited document is sent.

*0. If you want to add other work e.g. Google slides, drawings, go back to the 'Your work' section. Click on **+ Add or create**, which is under the document itself. You can add video or audio recordings easily in Slides or just add a file.*

Other Google applications

You can use your login and password to use:

- **Google Docs**
  - An online word processor like Microsoft Word
- **Google Slides**
  - An online presentation application like Microsoft PowerPoint
- **Google drive**
  - You can save work here to free up memory/space on your devices
  - You can store files on your Google Drive that you don't need to share with classmates
  - You can also access a shared drive that your year group can all access (for collaborative work)
  - How to move files into Google Drive. https://youtu.be/GQVGr_OM18Q