

Online safety policy

Jubilee Primary
School



Approved by: FGB **Date:** 22/09/2020

Last reviewed on: December 2018

Next review due by: 22/09/2023

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	7
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school	8
10. How the school will respond to issues of misuse	8
11. Training	8
12. Monitoring arrangements	9
13. Links with other policies	9
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	10
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	11
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	12
Appendix 4: online safety training needs – self audit for staff	13
Appendix 5: online safety incident report log	14
Appendix 6: Remote learning policy	15

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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 education and health education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department’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 co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 3)

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 and deputy/deputies are set out in our child protection and safeguarding policy as well 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- 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

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring 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.

3.6 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 1 and 2)

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 factsheet - [Childnet International](#)

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 3).

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](#).

From September 2020 **all** schools will have to teach:

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

This new requirement includes aspects about online safety. As such we've added these expectations in italics below, if your school isn't yet following the RSE 2020 guidance, please remove.

Primary schools insert:

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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

All schools - adapt this to reflect your school's approach:

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

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 or virtual learning environment (VLE Google Classrooms) This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

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. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 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

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

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

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

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

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

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 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

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

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Transferring data should whenever possible be done using google drive, if this is not possible, staff must use an encrypted USB drive.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

11. 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).

The DSL and deputy/deputies 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.

12. Monitoring arrangements

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

This policy will be reviewed every 3years by the School Business Manager At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- G-Suite policy
- Remote learning policy

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

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

Name of pupil:

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

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

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

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

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

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

Name of pupil:

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

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

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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

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

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

Signed (pupil):

Date:

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

Signed (parent/carer):

Date:

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

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

Name of staff member/governor/volunteer/visitor:

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

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

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

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

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

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

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

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

Date:

Appendix 4: online safety training needs – self audit for

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

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG			
Date	Where the incident took place	Description of the incident	Action taken

Appendix 6 Remote learning policy:

Contents

1. Aims.
2. Roles and responsibilities.
3. Who to contact
4. Data protection.
5. Links with other policies.

Aims

This remote learning policy for staff aims to:

- Ensure consistency in the school's approach to remote learning.
- Set out expectations for all members of the school community with regards to remote learning.
- Provide appropriate guidelines for data protection.

Roles and responsibilities

2.1 Teachers

In the event of a part or full school closure the school will revert to remote learning via the Google Apps for Education, Google Meet and Classroom apps.

Teachers must be available between 10am and 3.00pm. If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure. Please contact the office before 07.00am.

Teachers are responsible for:

- Setting up a remote learning timetable for their class to follow the agreed school timetable. Learning should include a mixture of face to face remote learning sessions through the 'Google Meet' app and additional activities set within the 'Google Classroom', appropriate to the age range you are teaching.
- Following the class timetable and planning and delivering lessons via either face to face remote learning sessions or activities set within the Google Classroom.
- All learning activities for the next day should be scheduled a day in advance where possible, to help facilitate learning in the case of absence or illness
- The Headteacher and senior members of staff including Lead teachers will be invited into your classroom. They can then support you and help answer any parental curriculum enquiries. The senior leadership team and subject leads will also monitor the learning content.
- Following the 'remote learning session' teacher protocols when delivering remote learning sessions.
- Remember to ensure that you are wearing professional dress for remote learning sessions and that you are working with a neutral background behind you.
- One to one remote sessions must be discussed and approved by the Headteacher to assess any risks. This could be required, to provide pastoral care or provide support for pupils with special educational needs and disabilities (SEND). Helpful solutions may involve including a parent or additional staff member on the call.
- Provide feedback to pupils about their work. This may be via comments in the Google Classroom, using Mote (chrome extension) or through the feedback section in google classroom.

- Work received via email is to be printed, marked, feedback given and then filed within a pupil's work folder.
- Ensure school email accounts are used for all correspondence.
- All emails received from parents should be answered during work hours.
- Any concerns or complaints must be shared with the Headteacher who will advise how to respond.
- For safeguarding concerns contact the DSL or DDSL and refer to the Child Protection and Safeguarding Policy and relevant sections below.
- Must ensure that throughout the week, welfare checks and call are being held with parents and recorded appropriately in the designated format.

2.2 Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Coordinating the remote learning approach across the school.
- Alerting teachers to resources they could use for remote learning.
- Working with teachers to make sure that the work set is appropriate and consistent.
- Monitoring the effectiveness of remote learning – Regular contact will take place with teachers through the Google Staffroom and staff meetings via the Google Meet app, reviewing work set conducting surveys for feedback from pupils and parents.
- Setting up and leading remote staff meetings.
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations.
- Keeping parents informed about Coronavirus update messages from the Government, the DfE and/or the Local Authority.

2.3 Designated safeguarding lead

The DSL will follow the guidelines set out in the addendum to the School's Child Protection and Safeguarding policy - COVID-19 School Closure arrangements for Safeguarding and Child Protection at Westward School.

Jubilee Primary School has two Designated Safeguarding Leads (DSL) and three Deputy DSL.

The Designated Safeguarding Leads are: Alia Zakir and Tom Prestwich

The Deputy Designated Safeguarding Leads are: Philippa Cail, Sam Esty and Alastair Crockett

Jubilee will have a trained DSL (or deputy) available on site. Where this is not the case a trained DSL (or deputy) will be available to be contacted via phone or online video - for example when working from home.

This might include updating and managing access to child protection systems and liaising with the offsite DSL (or deputy). It is important that all staff and volunteers have access to a trained DSL (or deputy). On each day, the staff on site will be made aware of who that person is and how to contact them.

The DSL will continue to engage with social workers, and attend all multi-agency meetings, which can be done remotely

2.4 Online Safety Coordinator

Alastair Crockett will be on hand to support both staff, parents and pupils with remote learning.

- Helping staff and parents with any technical issues they're experiencing.
- Reviewing the security of systems and flagging any data protection breaches to the data protection officer.
- Assisting pupils and parents with accessing the internet or devices.

- Ensuring online learning agreements have been signed by both parents, pupils and staff.
- Ensuring parents complete the correct paperwork if taking part in the Chromebook borrowing scheme.
- Emailing regular online safety messages to parents/carers to reinforce the importance of children staying safe online.

2.5 Pupils and parents

Staff can expect pupils to:

- Take part in the remote learning sessions provided by the class teacher.
- Complete work within the Google Classroom to the deadline set by teachers.
- Seek help if they need it, from teachers.
- Alert teachers if they're not able to complete work.

Staff can expect parents to:

- Make the school aware if their child is sick or otherwise can't complete work.
- Seek help from the school if they need it.
- Be respectful when making any complaints or concerns known to staff.

Who to contact

If staff have any questions or concerns, they should contact the following individuals:

If you have any issues with setting work, behaviour, own workload or well being please contact a member of the senior management team.

For issues with IT or concerns about data protection please contact either Brad Ekman or Alastair Crockett

For concerns about safeguarding please contact the DSL

Data protection

4.1 Accessing personal data

When accessing personal data, all staff members will work within their allocated Google account and drive.

4.2 Sharing personal data

Staff members may need to collect personal data such as email addresses as part of the remote learning system. While this may be necessary, staff are reminded to collect and/or share as little personal data as possible online. Staff should follow the school's GDPR protocols and the data protection policy and if unsure contact the DPO.

4.3 Keeping devices secure

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 recommended, a 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

Links with other policies:

- Online safety policy
- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- G-Suite policy

Appendix 1: remote learning plan

Remote Learning Plan

- There should be between 10 and 20 mins input (approx) of teacher input at the start of sessions - live using Google Meets. Teachers may also use Loom and Jam Board (which preloaded and extension programmes) in order to provide more personal resources which include their own voice to support the child's understanding.
- In EYFS the teacher-led section will be longer in most cases usually up to 20 minutes.
- Teachers can also use pre recorded slides and then talk through the slides with the children.
- After initial input the staff members stay on line so that if there are other questions they can be there.
- At the outset of a bubble or wider closure, teachers and additional adults should set expectations that the interaction is between children and teachers. Parental queries are to be typed and then time given to talk through issues after the scheduled lesson time has finished.
- Teachers should remind pupils that google meets, Loom and White Rose Maths lessons can be accessed later if the pupil was not online at the time.
- If you are delivering lessons live via Google Meets teachers should ensure you are recording your screen via either the recording function on Google Meets or the Loom extension so that pupils can watch back later. This also means that previous learning can be revisited at any time, to facilitate pre/ post teaching, that could be delivered as an intervention.

School day

YEARS 1-6

- 10:00-10:30 Reading Masters/Phonics
- 10:30-11:15 English
- 11:15-11:30 Break
- 11:30-12:15 Maths
- Lunch 12:15-1:00pm
- 1:15-Topic/Science/ Art/PE/Wellbeing including Circle Time
- 2pm-3pm allocated for reviewing learning, marking work handed in and response/feedback to pupils.
- 3 until 3:30 would be marking and feedback to individual pupils who need additional support

EYFS

- 10:00-10:30 Phonics
- 10:30-11:15 English
- 11:15-11:30 break
- 11:30-12:15 Maths
- Lunch 12:15-1:00pm
- 1:15-UW/EAD/ PD/ related to termly topic
- 2pm-3pm allocated for reviewing learning, marking work handed in and response/feedback to pupils.
- 3 until 3:30 would be marking and feedback to individual pupils who need additional support.

- Teachers need to complete the register on google sheets in the staff drive school closure folder.
- The office will collect email addresses so that parents can have a weekly update on what their child has accessed and handed in on google classroom each week. This should be automatically generated by google but we will confirm with you if this is applicable.
- Manipulatives, stationery and jottings books available in each classroom ready to go home in the event of a bubble closure.

SEN Pupils

- TAs and LSAs within each class will be directed to support individuals and groups of pupils with SEN needs. This may involve TAs and LSAs setting individual work or setting up their own virtual classrooms for their groups, providing additional contact to support the children during the whole class online learning, or more tailored online support via Google Meets. The provision for each SEN pupil will be tailored to their individual needs.

Wellbeing

- In the event of a lockdown - suggestions should be given to children for outdoor learning activities (that can be done in the park/on a balcony) - please speak to DSY if you need support for ideas about this. Please note this will not be possible during a bubble closure as children will need to self isolate in this instance.
- Classroom interactions should be monitored for children showing signs of anxiety. Any concerns by a teacher should initially be followed by a phone call home, and then referred to SLT (via email).
- Any family that has not logged into online learning will be followed up with by the office, but should also receive a wellbeing check in phone call from teachers. If teachers find they are unable to reach families please again refer to your phase AHT/DHT.
- Parents will be informed that they may request a phone call from a teacher if they have any concerns, this will happen via the office.
- We would encourage any staff member that is struggling with their own wellbeing during a closure to get in touch with a member of the SLT to discuss support that can be put into place.

Appendix 2 code of conduct:



Google Classroom

Tips for being a good classmate on Google Classroom

- Please join the Meet at the **correct time** & stay in the Meet for the entire time. If you are more than ten minutes late for the meeting then please do not join but watch the recording of the meeting which will be posted later in the morning.
- Find a quiet place away from distractions such as siblings, TV, pets, etc.
- Mute your microphone until you are called on to speak.
- If you are called on to speak, unmute your microphone so we can hear you.
- If you have a question, either raise your hand or put it in the chat.
- Keep the sidebar on chat.
- Please be respectful to others talking.
- The school's SMART 5 rules still apply as if you were in class.
- Do not take video recordings or screenshots/ photographs of the screen
- Hang up at the end of the Meet and do not attempt to rejoin until the next meeting.



Google Classroom

Tips for parents during live teaching on Google Classroom

- Check your safety / privacy settings are turned on.
- Please be aware that, from Wednesday, we will be recording the live teaching element of sessions so that families unable to attend a meeting will be able to watch it later in the classroom. Children's screens may be seen during this, but these recordings should not be shared outside of the children's classrooms.
- Remind children NOT to share passwords/ usernames with others.
- Ensure your children only log on at the time of the lesson and log out when it has ended.
- Whilst we do not require pupils to be in uniform, please ensure they are dressed ready for learning.
- If your child has been muted by their class teacher, please leave them on mute.
- Where possible, try to be close by to offer support if needed.
- When children are working independently, please allow them to do this- it is ok for them to make mistakes, it's all part of learning.
- As much as possible, please avoid asking teachers questions during the live learning, if you have a learning query please type it in the chat bar or wait until the feedback session in the timetable.
- As much as possible, avoid having separate conversations with

others in the same room as this can be a little distracting for others.

- Do not take or allow your child to take video recordings or screenshots/ photographs of the screen.
- Please ensure your child logs in under their google account, not a personal one.
- If you are unsure of any safety rules, please ask.



Google Classroom

Online learning and School Closure Guide for Staff

- Only login using your school account.
- Do not admit anyone to the Google Classroom who is trying to enter using an external account. If you recognise the address as a family member of a child, please make contact with them and let them know they need to enter via the child's school account.
- When working from home, where possible, use a room that isn't a bedroom, or use a blurred background to keep your home obscured.
- Avoid one to one conversations online with children (unless previously agreed by SLT) and only communicate with children online during school hours (marking of work may take place outside of school hours, but please consider your own wellbeing when completing this work at this time).

- Record all core subject live lessons (up to the point when children start working independently) and post in the classroom with the lesson as soon as possible so that children who were not able to join the live meet are able to view it in their own time.
- Please obscure the meet code, only make the room available once you are inside as then you will have host controls. Please then reset the meet code at the end of every online meet, both of these functions can be found in settings (the small cog).
- The safeguarding policy is still the same, all concerns must be logged on Edukey and any “yellow form” concerns must be reported to Tom Prestwich or Alia Zakir as soon as possible.
- Wellbeing phone calls should be carried out for all children/families at least once a week (dated notes to be put onto the “Communication with Families During Closure” form). Where you are struggling to make contact with a family, this should be raised at the weekly phase meeting so a member of the SLT can attempt to make contact also.

Appendix 7:

