Abbots Farm Junior School Online Safety Policy Addendum (in relation to remote learning)

Introduction

This addendum has been created following DfE guidance Actions for schools during the coronavirus outbreak (Full Opening: Schools). It is an addendum to the School's Online Safety Policy and procedures and must be read in conjunction with the Online Safety Policy, Acceptable Use Policy, Relationships Policy, Safeguarding policy and (for staff and other adults) the Code of Conduct for Staff (including any Addendums to these). The school's Online Safety Policy along with this Addendum is available on request and must be read and understood by all those individuals involved in providing remote education for the children of Abbots Farm Junior School.

All staff have a responsibility to be aware of systems within school which support safeguarding and any temporary amendment to these will be explained to them by SLT. This includes the school's Child Protection Policy and procedures, the school Code of Conduct or Staff Behaviour Policy, the Online Safety Policy and the associated Acceptable Use Agreements.

Context

From 6th January 2021, once again, parents were asked to keep their children at home, wherever possible, and for schools to remain open only for those children classed as vulnerable and children of workers critical to the Covid-19 response, who absolutely need to attend. Schools have been expected to deliver a cohesive Remote Learning curriculum for those at home.

Despite the changes, **our Online Safety Policy is fundamentally the same** with this addendum setting out some of the adjustments we are making in line with the altered arrangements and following advice from government and local agencies.

This Addendum will be reviewed regularly as the nature of the pandemic and local or national responses that involve remote education, or government guidance on how we should operate significantly changes.

Once adopted, this Addendum may be referred to in any disciplinary proceedings following unacceptable action by staff or other adults.

Online Safety and Remote Education

During periods of lockdown in a pandemic, whether experienced by the whole community if Public Health advises us to close, or by individuals who become ill or receive a positive test result for Covid-19 or must self-isolate because they have come into close contact with someone who has, learning will move substantially online for most pupils.

Our Policies, procedures and supporting documents like our Acceptable Use Policies have been reviewed to ensure they reflect how we will manage remote education and that they remain appropriate and useful for keeping people safe online during a pandemic.

Where a class, group or small number of pupils need to self-isolate, or there is a local lockdown requiring pupils to remain at home, we will ensure we have the capacity to offer **immediate** remote education. Please refer to our AFJS Remote Education Plan for further details.

School has assessed the increase in risk presented by remote learning specific to our setting, in line with Government and Local Authority guidance. The main additional issues to address are outlined in **3.1 (Equality)** and **3.2 (Safeguarding)**:

3.1 Equality of access to remote education

School will utilise any allocation of devices provided by the DfE Laptops for Disadvantaged Children Programme and will follow advice from the DfE guide Get help with technology.

Before distributing devices, school will ensure:

- They are set up to access remote education.
- Appropriate safeguarding controls and support are in place to help children and families use devices safely.
- Parents are aware of the device loan scheme details, including: length of loan agreement, who owns the devices, responsibilities of borrowers, how loss, theft or damage is managed, and repair or replacement arrangements for faulty devices under warranty.

Information is, or will be, made available to parents and carers about:

- Connectivity support available for disadvantaged children through increased mobile data allowances.
- Keeping children safe online DfE guidance and other support materials available

3.2 Safeguarding during remote education

We recognise the additional risks to pupils associated with being online more than before the pandemic, helpfully summarised by the South West Grid for Learning (SWGfL) report.

We also recognise additional risks for staff, especially those facilitating remote learning via video links, that may impact other people in their household or community as well. As set out in the Coronavirus (COVID-19): safeguarding in schools, colleges and other providers guidance, online education should follow the same principles

3.2.1 Protocols for staff in relation to remote education

- Only use school approved platforms; do not use social media to communicate with pupils
- Reinforce online safety messages regularly in your teaching
- Bear in mind the current circumstances and how they are affecting children and families when setting expectations of pupils
- Consider online safety when sharing resources – vet websites and videos/apps/software carefully and bear in mind that the home environment will not have the same content filtering systems as at school.
- Do not introduce any new apps and resources without the approval of SLT
- If concerned about online safety, check with the Online Safety Lead (DHT) or the Headteacher
- Ensure that passwords and secure information, such as logins for CPOMS, are kept confidential
- Adhere to copyright and GDPR guidelines
- Continue to look out for signs that a child may be at risk, which may differ from typical triggers in a school environment. Report any concerns to a DSL without delay in the usual way – if working from home and unable to complete a green form, make telephone contact with school and speak to a DSL.

- Do not provide pupils or parents with personal contact details (email, home or mobile numbers, details of web-based identities etc.)
- Do not arrange to meet students or ask them to deliver work to your home
- Remain professional and objective in all emails and other forms of correspondence

When conducting live sessions (staff)

- Keep a record/log of live online sessions – date and time, attendance, what was covered, any incidents. Any serious incidents should be reported in the usual manner.
- Follow the AFJS Live Sessions Expectations document
- Maintain professional conduct
- Ensure that you have no other tabs open on your browser, particularly if you are sharing your screen
- Maintain the same boundaries and insist on the same standard of behaviour as in a school setting.
- Make specific protocols clear at the outset, e.g. all pupils switch off their camera, mute microphones at appropriate times, use of the chat function, etc.

When participating in live sessions (pupils)

- Always log on through the link sent to your parents
- Do not make recordings, take screenshots/screengrabs or photographs, or store footage of teachers or other pupils
- Ensure that you have a safe and appropriate place to participate from. If not, please inform your teacher immediately
- Follow the school rules for conduct during online lessons as if you were in school
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust

We will follow relevant government safeguarding guidelines and make use of recommended technical tools and guides to help us deliver remote education safely from organisations like The Key for School Leaders, and education and child protection specialists like SWGfL, London GfL and the NSPCC.

In addition to the updated codes of conduct, staff, pupils (or due to their age and ability, the adults supporting them), parents, carers, and to some degree, virtual or in-person visitors using online technology for education purposes or school business, are expected to (with support where required):

Check security and privacy settings

- Adjust privacy and safety settings on all devices, in apps and other online places to control what personal data is shared.
- Review the security settings on 'smart' devices and change any default, weak or guessable passwords.
- Set up two-factor authentication if devices are capable or available. This is a free security feature to stop unwanted people getting into accounts. Users receive a text or code when they log in to check they are who they say they are.
- Regularly update devices or apps used for school or work. Using the latest version of software and apps can immediately improve security.
- Think about physical privacy when appearing live/in pre-recorded videos online e.g. appropriate clothing, distractions like noise and interruptions, what other people nearby can hear, the appropriate adult supervision of children at home. See our *AFJS Live Sessions Expectations* document for further details on this.

Act regarding unsuitable content

- Prevent unwanted content from appearing i.e. set filters and parental controls on home broadband and mobile networks and not disable or bypass them (the UK Safer Internet Centre has advice on how).
- Block unsuitable contact (with support as necessary)
- Report harmful activity, to the website, platform or app, a trusted adult and the Designated Safeguarding Lead with responsibility for Online Safety in school (DHT in the first instance). Report Harmful Content to Safer Internet UK if not satisfied with the result of a report to a service provider.

Stay physically and mentally healthy online

Whether staff or pupils are working, learning or playing online, they should take regular breaks and use tools like Apple's Screen Time or Google's Family link if necessary, to manage screen time, especially:

- if they're feeling overwhelmed, frustrated or worried
- if they're feeling physical discomfort like aches, pins and needles, pain, strain, headaches; or
- if they need to be more physically active outdoors.

Parents and carers will be given guidance on supporting their child's mental health and wellbeing during COVID-19 as well as screen time advice from the Chief Medical Officer. We will also provide practical guidance on making the home environment a good and safe one to learn in with a sensitive appreciation for people's different home circumstances and what is reasonable.

Staff are also expected to:

- Provide information about their temporary home working environment if it might impact on their physical health, or the safeguarding of learners or their own household
- Act appropriately on feedback and use any necessary online tools provided
- Provide information about the technology they use at home to get online i.e. to ensure compatibility with school systems, especially cyber security measures involved in accessing sensitive data like medical, behaviour or performance information on school servers remotely
- Implement relevant guidance on safe teaching and pastoral care from their home e.g. what is in the background of recorded or live streams, what is visible on shared screens, what can be heard by others in a household etc
- Pay special attention to how they protect personal data at home

Keep talking about staying safe online

It is important to continue to remind children of the online safety messages we regularly promote in school and which are detailed within our AFJS Acceptable Use Policy.

- Ensuring staff have the tools to promote a healthy balance between the positive and negative aspects of life online.
- Signposting parents and carers to tools to explain and reduce risks, and help them talk to their child (e.g. UKCIS guidance on minimising children's exposure to risks; Childnet International's conversation starters; Ditch the Label teacher resources that can be helpful for parents to discuss cyberbullying; the government's helpful advice; and where there are concerns about specific serious harms, the guidance on how to protect your child from child sexual abuse online, 'sexting' or radicalising, pornographic or suicide content)
- Reiterating behaviour expectations and ways to handle and report problems, especially encouraging children to speak to a trusted adult if they come across content online that makes them uncomfortable.
- Supporting critical thinking and promoting resources like Parent Zone's guide and Childnet's advice and top tips which provide ways parents and carers can help their child develop these skills.

3.3 Reporting concerns and receiving online safety support during remote education

Reporting an issue for staff:

- Any child protection or safeguarding concern must be reported to the safeguarding Team without delay and entered on a cause of concern form on CPOMS or in the unlikely event that the Safeguarding Team is unavailable, all concerns must be reported to the Headteacher.
- Concerns about the safety of procedures, behaviours or use of technology should be referred to the DSL

Reporting an issue for pupils:

- Speak to a trusted adult at home or send a message to your teacher via Seesaw
- Contact Childline 0800 1111 or click CEOP https://www.ceop.police.uk/safety-centre/

Reporting an issue for parents:

- If you have any worries or concerns about the welfare of your child, please contact school for any safeguarding or child protection or online safety concerns
- You can also report an incident to CEOP (Child Exploitation Online Protection) https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/parents/Gethelp/Reporting-an-incident/ or Report Harmful Content https://reportharmfulcontent.com/
- Please contact your child's class teacher in the usual way (admin2421@welearn365.com)for routine queries about remote learning

3.4 The role of parents in supporting online safety during remote education

It is the responsibility of parents to ensure that pupils are monitored in their use of technology for Online Remote Learning as they would ordinarily do when their children are using technology at home. Monitoring screen time is particularly important in the current circumstances

While pupils are working from home, they are connected to their home broadband, so their traffic doesn't go through the AFJS firewall. Parents will therefore need to ensure that age-appropriate filtering or safe search is enabled at home. Information on setting this up can be found at:
https://www.saferinternet.org.uk/advice-centre/parents-and-carers
https://www.internetmatters.org/parental-controls/

Communication on Seesaw during online learning is between pupil and teacher: parents should communicate with school/staff in the usual manner, via the school admin email: admin2421@welearn365.com or by telephone during any period of remote learning.

Any parent wishing to supplement the school's remote learning with support from online companies or individual tutors should be mindful of the importance of using reputable organisations or individuals who can provide evidence that they are safe and can be trusted to have access to children.

Social media, networking apps and gaming platforms are particularly popular at the moment. Parents are responsible to be mindful of age restrictions and to oversee their child's social media activity.

The school will update parents regularly on online safety matters. Parents are requested to heed the school's advice and contact the school if they have concerns or encounter risk online as detailed in section 3.3 above.