Akaal Primary School

Online Safety Policy

Approved by:	Safeguarding Cttee	**Date:** 27th February 2020
Last reviewed on:	January 2020	
Next review due by:	November 2021	

Contents

1. Aims

Akaal Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors and visitors
- 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
- To deliver an I.T. curriculum which covers a wide range of different technology, its uses, and how it is to be used appropriately.

2. E-Safety

At Akaal Primary we recognize the range of e-safety issues and plan accordingly to help ensure the appropriate, effective and safe use of electronic communications within our school.

E-Safety encompasses not only internet technologies but also electronic communications such as mobile phones, tablets, mobile devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their safety and that of others.

- Why Use the Internet in School?
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, enhance communication, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

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 DSL 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 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.

3.5 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

3.6 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. 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

5. Educating pupils about online safety

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

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*

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.

The school uses personal development sessions to raise awareness of e-safety and the issues that surround it

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 My School App. 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 classes at an age appropriate level, 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. Cyber-bullying also comes in the E-safety topic in our school's personal development sessions.

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

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

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

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

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. 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 Online Safety and Behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

8. School Website

The school has developed its own website that contains information about the ethos and values of the school, the staff and other relevant information including recent newsletters. The website is updated on a regular basis and the content is reviewed regularly to ensure that it is well presented and that personal security is not compromised. The school takes the following precautions to ensure the security of its staff and pupils is maintained:

- All materials published are monitored by the Headteacher and/or IT Coordinator;
- The website and Facebook page contains names of individual members of staff, but individuals cannot be identified from photographs and no information relating to home addresses or individual e-mail identities are published;
- Named photographs of pupils are not published on the web site. Any group photographs do not have a name list attached.
- Wherever possible, photographs with smaller images of children are used to minimize identification of individual children;
- Checks are made that all pupils in photographs are appropriately clothed;
- Parental permission is obtained for all pupils whose photographs appear on the website. Additional permission is obtained regarding use of the child's photograph in local media;
- The point of contact on the website and Facebook is the school address, telephone number and e-mail address;
- Pupils are encouraged to share their ideas and views using only closed and controlled forums and discussion groups. Any inappropriate content will be removed immediately and an appropriate sanction taken.

9. Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. For use by responsible individuals, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content.

Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. Examples include: blogs, wikis, Instagram, Facebook, Twitter, Whatsapp, Snapchat, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

The school recognises the increasing value of social networking and personal publishing but takes the following precautions to ensure safety: -

- Conferencing will only be permitted to a known group of users, that has been selected and approved by the class teacher;
- Social networking sites will not be made available to pupils unless an educational requirement for their use has been demonstrated;
- Wherever possible, forums, blogs etc are encouraged via a recognised educational provider which has a restricted audience and can be managed by the school. Entries will be monitored closely by the creator of the forum and any mis-use will be reported to the IT Coordinator;
- Pupils will not be allowed access to public or unregulated chat rooms;
- Children are only permitted to use regulated, educational chat rooms. This use is supervised and the importance of chat room safety emphasised;
- Pupils are advised not to place personal photos on any social network space.
- Pupils are reminded never to reveal personal details of themselves, friends or family without checking first with a responsible adult;
- Pupils are reminded that users may try to assume a different identity and that all communication should be done with caution. Similarly, pupils should never pretend to be someone else or steal their identity;
- All pupils are advised to talk to a responsible adult if they suspect that a site is being used inappropriately;
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

10. Video Conferencing

Video conferencing enables users to see and hear each other between different locations. It is a real time, interactive technology and has many uses in education. Equipment ranges from small PC systems (web cameras), tablets, mobile devices (including Skype and Facetime, to large room based systems that can be used for whole classes or lectures. The video conferencing equipment uses a network to communicate with the other site.

The school takes the following precautions to ensure the safety of staff and pupils:

- All video conferencing uses the broadband network to ensure quality of service and security rather than the Internet;
- All video conferencing equipment in the classroom is switched off when not in use and not set to auto answer;
- External IP addresses are not made available to other sites;
- Video conferencing contact information is not put on the school website;
- Equipment is secured and locked away when not in use;
- School video conferencing equipment is not taken off school premises without permission as use over the non-educational network cannot be monitored or controlled;
- Pupils should ask permission from the supervising teacher before making or answering a video conference call;
- Video conferencing is always supervised appropriately;
- Dialogue is established with other conference participants before taking part in a video conference. Measures are taken to check that materials to be delivered are appropriate for the age group of participants;

- Unique log on and password details for the educational videoconferencing service are only issued to members of staff and kept secure.

11. Emerging Internet Applications

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide Internet access and multimedia present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. When considering the use of any new technology, the school applies the following principles:

- Emerging technologies are examined for educational benefit;
- A risk assessment is carried out before use in school is permitted;
- Pupils are reminded about safe practices and responsibilities;
- Use of the technology is monitored and regulated.

12. Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The General Data Protection Regulations (GDPR) which came into force in May 2018 applies to anyone who handles or has access to information concerning individuals.

- Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).
- The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:
    - Processed fairly and lawfully
    - Processed for specified purposes
    - Adequate, relevant and not excessive
    - Accurate and up-to-date
    - Held no longer than is necessary
    - Processed in line with individuals rights
    - Kept secure
    - Transferred only to other countries with suitable security measures.
- All Personal data is recorded, processed, transferred and made available according to the GDPR regulations effective from May 2018.

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

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

Name of pupil:

When I use the school's ICT systems (like computers or any electronic device) 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: Akaal Primary School, KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

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

Name of pupil:

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

When I use the school's ICT systems (like computers or any electronic device) 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: Akaal Primary School acceptable use agreement (staff, governors, volunteers and visitors)

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

Name of staff member/governor/volunteer/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school’s reputation
- Access social networking sites or chat rooms; however this does not include those of a professional nature and related to my working responsibilities, or those used as part of the school’s public promotion tools.
- 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
- I will only take photographs of pupils as part of learning or for assessment purposes, and even then I will adhere to advice contained in “Safer Working Practices”.
- 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: Akaal Primary School online safety training needs – self-audit for staff

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: Akaal Primary School online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**