Online Safety Policy

Version Control

Version	**V1.1**
Ratified by	Governors
Owner	**Hannah Shutt**
Date Issued	**March 2023**
Review Date	**Spring Term 2024**
Target	All Stakeholders

Change History

Version	Owner	Change Summary	Document Date
V1.1	**Julie Cordingley**	Additional section added and self-audit appendix 4 amended to include sharing of nudes and semi-nudes	**November 2021**
V1.1.	**Hannah Shutt**	**Reapproved**	**March 2023**

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff(including part-time workers and students), 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, Online Safety (Annex C) in recognition that 'the use of technology has become a significant component of many safeguarding issues.' This could include issues such as child sexual exploitation and radicalisation – 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 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).

The governor who oversees online safety is Ira Jeffers

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 deputies 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, 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 regular 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, students 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:

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. All children will take part in Safer Internet Day annually.

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.

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 in an age appropriate manner. Class teachers will discuss cyber-bullying with their class, 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 they must be turned off on entry to the school grounds and kept in the school office during the day.

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. Sharing nudes and semi-nudes: responding to an incident

Sharing nudes and semi-nudes this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may be used.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

If an incident comes to the attention of an adult working in school:

Report to school's Designated Safeguarding Lead – Tamsin. The school's Safeguarding and Child protection policy outlines the practice to be followed.

Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.

Do not delete the imagery or ask the young person to delete it.

Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).

Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
Do not say or do anything to blame or shame any young people involved.

Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

10. Staff (including students) 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. Any USB devices containing data relating to the school must be encrypted. It is highly recommended that all staff store work related documents on Onedrive.

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.

11. 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 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 school disciplinary policy. 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.

12. 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 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.

13. Filtering and Monitoring Systems

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible. The school broadband is provided by School Broadband, who provide filtering through the filtering company Netsweeper.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

Duty for School under Counter Terrorism and Securities Act 2015 Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet

along with other potential harms. The school receives a daily Prevent Alert report form the school broadband provider which is checked each day by the Headteacher.

The school has provided enhanced user-level filtering, allowing different filtering levels for different groups of users, i.e. staff and pupils. School staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.

14. Monitoring arrangements

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

This policy will be reviewed at a minimum of every two years by the PSHE Lead in conjunction with the DSL, however regular review will take to reflect the nature of rapidly changing technology developments and consequent evolving risks including those from **radicalisation**, CSE and other online harms to inform the training needs of young people and staff.

Following review this policy will be shared with the governing board.

15. 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
- Prevent Strategy
- **Counter Terrorism and Securities Act 2015** (Statutory Prevent Duty - which requires schools to ensure that children are safe from terrorist and extremist material on the internet)

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

Adel Primary School

Acceptable Use Agreement for Early Years pupils

- I will look after the school's equipment and use it properly.
- I will ask for help from a teacher or other adult if I don't know what to do or if I think that I have done something wrong.
- I will only share my username or password with trusted adults (my teacher or parent).
- I will ask permission from a teacher before using the internet and will only use websites that I am allowed to visit.
- I will not write anything that upsets other people.
- I will only take a photo or video of someone if they say it's OK.
- If I see anything that upsets me or that I do not like, I will tell a teacher.
- I understand that my teacher may talk to my parent or carer if they are worried about my use of school IT equipment.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while.

Name of Pupil:

Please sign here after reading this through with your child:

Relationship to child:

As the parent / carer of the above student, I give permission for them to have access to the internet and to ICT systems at school.

I understand that their use of ICT will be monitored and that the school will contact me if they have concerns.

I will encourage my child to use the internet and technology safely at home and will talk to the school if I have any worries about my child's online safety or the safety of his or her friends.

I understand that my child has received – and will continue to receive – online safety education to help them understand how to use technology safely in and outside of school.

Parent / Carer's Name _____

Signature _____

Date _____

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

Adel Primary School

Acceptable Use Agreement for primary school students

Technology is an important part of school life. These rules are here to help keep you, your friends and your family safe. When you sign this form you are agreeing to follow these rules when you are using the school computers, tablets, email, digital cameras and other ICT.

- I will only use the school's computers for schoolwork and homework.
- I will ask for help from a teacher or other adult if I don't know what to do or if I think that I have done something wrong.
- I will keep my login and password secret.
- I will not bring computer files or games into school without permission.
- I will ask permission from a teacher before using the internet and will only use websites that I am allowed to visit.
- I will only email people I know, or that my teacher has approved.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not post my home address, phone number, send a photograph or video, or give any other personal information about myself or my friends and family unless my teacher has given permission.
- If I see anything that upsets me or that I do not like, I will not respond to it but I will tell a teacher or parent.
- I will only use my own technology (e.g. mobile phone or tablet) in school when I have permission to do so.
- I will tell a teacher if I am worried about something another pupil asks me to do.
- I will tell a teacher if I am worried about something my friends are doing online.
- I will be act responsibly when using technology both in and out of school, including when sharing of images or data.

Class

Name of Pupil

Your signature

As the parent / carer of the above student, I give permission for them to have access to the internet and to ICT systems at school.

I understand that their use of ICT will be monitored and that the school will contact me if they have concerns.

I will encourage my child to use the internet and technology safely at home and will talk to the school if I have any worries about my child's online safety or the safety of his or her friends.

I understand that my child has received – and will continue to receive – online safety education to help them understand how to use technology safely in and outside of school.

Signed _____

Parent / Carer's Name _____

Date _____

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

Adel Primary School

Acceptable Use Agreement for staff, governors, students and volunteers

Technology is a valuable tool for education and an important part of our pupils' lives. We encourage the use and teaching of ICT. All members of staff (including part time workers, students, governors and volunteers) are responsible for helping us maintain user safety and the school's reputation, as well as fulfilling any legal requirements.

This Acceptable Use Policy (AUP) is part of our induction process. We also ensure that all staff and volunteers receive regular and up to date training and information on all issues related to use of ICT in the school.

It is important that all our members of staff are aware that their behaviour online both in and out of school can have an impact on their role and reputation, and the reputation of the school. All staff must read, understand and sign this Acceptable Use Policy before being given access to any of the schools' ICT systems.

Our Acceptable Use Policy has been developed to ensure that:

- All members of staff are fully aware of their professional responsibilities when using ICT and the school systems.
- Our ICT systems and users are protected from accidental or deliberate misuse that could put the security of our systems and users at risk.
- All staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

Acceptable Use Policy Agreement

This is not an exhaustive list and all staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the law.

- I understand that the term ICT include networks, data and data storage, online and offline communication technologies and access devices and includes use of mobile phones, tablets and social networking sites.
- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure my compliance with this policy.
- I have read and understood the online safety policy.
- My use of ICT will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work and will be in accordance with the school Acceptable Use Policy and the law.

- My electronic communications with pupils, parents/carers and other professionals will only take place via a school email address or school telephone number and I will communicate in a professional manner at all times.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password and ensure that I log out correctly from any systems after use.
- I will not install any purchased or downloaded software or hardware without permission from the system manager. In addition, I will not open hyperlinks or attachments in emails unless they are from a trusted source.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988 and EU General Data Protection Regulation (GDPR) 2018. Any images or videos of pupils will only be used as stated on the 'photograph/video permission' slips that have been signed by parents and will always take into account parental consent.
- I will not store documents that contain school-related sensitive or personal information on any personal devices unless they are secured and encrypted. I will protect the devices in my care from unauthorised access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the designated person as soon as possible.
- I will not create, upload, download, access or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

I have read and understood the above, and agree to use the school ICT systems and devices within these guidelines. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Signed _____

Print Name _____

Approved by _____

Date _____

Appendix 4: 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?	
Do you know how to respond to an incident where nudes or semi-nudes have been shared by young people under the age of 18?	
Are there any areas of online safety in which you would like training/further training?	

Equality Impact Assessment

		Yes/ No	Comments
1.	**Does the policy / guidance affect one group less or more favourably than another on the basis of:**		
	▪ **age**	No	
	▪ **disability**	No	
	▪ **gender reassignment**	No	
	▪ **marriage and civil partnership**	No	
	▪ **pregnancy and maternity**	No	
	▪ **race**	No	
	▪ **religion or belief**	No	
	▪ **sex**	No	
	▪ **sexual orientation**	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the policy/ guidance likely to be negative?**	No	
5.	**If so, can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/ guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	