Online Safety Policy

Table of Contents

1. Aims

Alfred Lord Tennyson School (ALTS) 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 [1], and its advice for schools on:

- Teaching online safety in school [2]
- Preventing and talking bullying and cyber bullying: advice for Headteachers and school staff [3]
- Searching, screening and confiscation [4]

It also refers to the Department's guidance on Protecting Children from Radicalisation [5].

It reflects existing legislation, including but not limited to the Education Act 1996 [6] (as amended), the Education and Inspections Act 2006 [7]and the Equality Act 2010 [8]. In addition, it reflects the Education Act 2011 [9], 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 Safeguarding Governor will co-ordinate regular meetings, twice a year, 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 (0)

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 are set out in our Child Protection and Safeguarding Policy [10] 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 4) 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 [11]
- Liaising with other agencies and/or external services if necessary

3.4. The ICT Subject Lead / ICT Technician

The ICT Subject Lead 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 weekly 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 4) 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 [11]

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 (Appendix 1 and Appendix 2)
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) 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 [11]

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 (Appendix 1 and Appendix 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 [12]
- Hot topics - Childnet International [13]
- Parent factsheet - Childnet International [14]

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 (0).

4. Educating Pupils About On-Line Safety

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

- National Curriculum computing programmes of study [15].
  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
- The ALTS PSHE (Personal, Social, Health Education) Policy [16].
  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.

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.

6. Cyberbullying

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 and Anti Bullying Policy** [11]**.**)

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. 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 [11]. 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 [7] (which has been increased by the Education Act 2011 [9]) 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 [17].

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school Complaints procedure [18].

7. Acceptable Use

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 (11Appendix 1, Appendix 2, Appendix 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 Appendix 1, Appendix 2 and Appendix 3.

8. Mobile Phones

Pupils may bring mobile devices into school, but are not permitted to use them whilst in school – a permission letter must be signed by parents and phones must be left in the school office:

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. See Mobile Phone Policy [19] for further information.

9. Staff Using Work Devices Outside of 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 0.

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.

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. 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 [20]. 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. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 4.

This policy will be reviewed every two years by the Computing subject lead. At every review, the policy will be shared with the Governing Board.

12. Links with Other Documentation

This online safety policy is also linked to:

- Staff Disciplinary procedures [21]
- Data protection policy and privacy notices [22]
- Complaints procedure [23]
- PSHE and RSE Policy [16]
- Anti Bullying Policy [24]

- ICT Acceptable Use Policy [25]

[1] gov.uk, “Keeping children safe in education,” 2 April 2020. [Online]. Available: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2. [Accessed 6 May 2020].

[2] gov.uk, “Teaching online safety in schools,” 26 june 2019. [Online]. Available: https://www.gov.uk/government/publications/teaching-online-safety-in-schools. [Accessed 26 June 2020].

[3] gov.uk, “Preventing bullying,” 4 July 2017. [Online]. Available: https://www.gov.uk/government/publications/preventing-and-tackling-bullying. [Accessed 26 June 2020].

[4] gov.uk, “Searching, screening and confiscation at school,” 18 January 2018. [Online]. Available: https://www.gov.uk/government/publications/searching-screening-and-confiscation. [Accessed 26 June 2020].

[5] gov.uk, “Protecting children from radicalisation: the prevent duty,” 17 August 2015. [Online]. Available: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty. [Accessed 28 June 2020].

[6] legislation.gov, “Education Act 1996,” 1996. [Online]. Available: https://www.legislation.gov.uk/ukpga/1996/56/section/444. [Accessed 7 May 2020].

[7] legislation.gov.uk, “Education and Inspections Act 2006,” [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/40/part/7/chapter/2. [Accessed 12 May 2020].

[8] legislation.gov, “Equality Act 2010,” 2010. [Online]. Available: https://www.legislation.gov.uk/ukpga/2010/15/contents. [Accessed 4 May 2020].

[9] legislation.gov.uk, “Education Act 2011,” [Online]. Available: https://www.legislation.gov.uk/ukpga/2011/21/contents/enacted. [Accessed 12 May 2020].

[10] Alfred Lord Tennyson School, “Child Protection and Safeguarding Policy,” 2020.

[11] Alfred Lord Tennyson School, “Behaviour Policy,” 2020.

[12] UK Safer Internet Centre, “What are the issues?,” [Online]. Available: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues. [Accessed 28 June 2020].

[13] Childnet International, “Hot Topics,” [Online]. Available: http://www.childnet.com/parents-and-carers/hot-topics. [Accessed 28 June 2020].

[14] Childnet International, “Parents and Carers resource sheet,” [Online]. Available: https://www.childnet.com/resources/parents-and-carers-resource-sheet. [Accessed June28 2020].

[15] GOV.UK, “National curriculum in England: computing programmes of study,” 11 September 2013. [Online]. Available: https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study. [Accessed 2020 June 2020].

[16] Alfred Lord Tennyson School, “PSHE and RSE Policy”.

[17] gov.uk, “Searching, screening and confiscation at school,” 18 January 2018. [Online]. Available: https://www.gov.uk/government/publications/searching-screening-and-confiscation. [Accessed 28 June 2020].

[18] Alfred Lord Tennyson School, “Complaint Policy”.

[19] Alfred Lord Tennyson School, “Mobile Phone Policy,” 2018.

[20] Alfred Lord Tennyson School, “Staff Code of Conduct,” 2020.

[21] Alfred Lord Tennyson School, “Staff Disciplinary Policy,” 2020.

[22] Alfred Lord Tennyson School, “GDPR Policy 2018”.

[23] Alfred Lord Tennyson School, “Complaint Policy 2019”.

[24] Alfred Lord Tennyson School, “Anti-Bullying Policy 2019”.

[25] Alfred Lord Tennyson School, “ICT Acceptable Use Policy,” 2020.

[26] GOV.UK, “Education Act 1996,” 1996. [Online]. Available: https://www.legislation.gov.uk/ukpga/1996/56/contents. [Accessed 19 February 2020].

[27] legislation.gov.uk, “Data Protection Act 2018,” 2018. [Online]. Available: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [Accessed 12 November 2020].

[28] gov.uk, “Guide to the General Data Protection Regulation,” 25 May 2018. [Online]. Available: https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation. [Accessed 12 November 2020].

[29] legislation.gov.uk, “Computer Misuse Act 1990,” 1990. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents. [Accessed 12 November 2020].

[30] legislation.gov.uk, “Human Rights Act 1998,” [Online]. Available: https://www.legislation.gov.uk/ukpga/1998/42/contents. [Accessed 12 May 2020].

[31] legislation.gov.uk, “The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,” 2000. [Online]. Available: https://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made. [Accessed 12 November 2020].

[32] legislation.gov.uk, “Freedom of Information Act 2000,” [Online]. Available: https://www.legislation.gov.uk/ukpga/2000/36/contents. [Accessed 1 July 2020].

[33] legislation.gov, “Education and Inspections Act 2006,” 2006. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/40/contents. [Accessed 4 May 2020].

13. Safeguarding

Safeguarding our children is our priority – see Child Protection and Safeguarding Policy [10]. All concerns must be reported to our Designated Safeguarding leads:

Mrs K O’Connor, Mrs S Smith Mrs J Appleby and Mrs L Bunker

Appendix 1. Acceptable use agreements for parents/carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: …… **Name of child:……**	
Online channels are an important way for parents/carers to communicate with, or about, our school. • The school uses the following channels: • Our official Facebook page Email/text groups for parents (for school announcements and information) Our virtual learning platform – Purple Mash	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way I will contact the school and speak to the appropriate member of staff if I have any complaints or concerns. • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed: ……	**Date: ……**

Appendix 2. Acceptable use agreements for pupils, staff parents/carers)

Acceptable use of the school's ICT facilities and internet: agreement for pupils	
Name of pupil:……	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
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 3. Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member / governor / volunteer / visitor:	.....

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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
- 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 understand 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)**	.....

Appendix 4. 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