Adelaide Primary School

E-Safety Policy

Respect – Equality - Effort

"Our vision is to provide all of our children with a body of knowledge, skills and vocabulary alongside the development of an exceptional character so that they thrive and succeed in all that they do!"

Reviewed: September 2026

Next review: September 2027

Adelaide Primary School

E-Safety Policy

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

- Users - refers to all staff, pupils, governors, volunteers and any other person working in or on behalf of the school, including contractors.
- Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
- School – any school business or activity conducted on or off the site, e.g. visits, conferences, trips etc.

Safeguarding is a serious matter; at Adelaide Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e- safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Adelaide website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each academic year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school's technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher (K Bradley)

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate training in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.
- The school's filtering and monitoring systems are reviewed at least annually. The review will be undertaken by the member of the Senior Leadership Team responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT Support. Records of the review and any actions arising will be retained.

Designated Safeguarding Lead / E-Safety Officer (M Anthony)

The Designated Safeguarding Lead (DSL) should take the lead responsibility for safeguarding and child protection, including e-Safety, as per Keeping Children Safe in Education. However, the DSL may delegate certain e-Safety functions to other members of the school eg ICT Support Services.

The day-to-day duty of e-Safety Officer is devolved to Meg Anthony (DSL & Deputy Headteacher & Kirsten Bradley (Headteacher).

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in the school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Ensure that filtering and monitoring systems are effective, regularly reviewed and aligned with current safeguarding requirements, including emerging online risks.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.

    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
- Passwords are applied correctly to all user accounts adhering to complexity settings. Age-appropriate passwords are set for pupils by the class teacher, or administrator.
- Passwords for staff will be a minimum of 8 characters.
- Staff passwords will expire every 42 days, and a new unique password must be selected.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in their absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision.
- All online material is checked fully before using either within the classroom or remotely
- The DSL is informed if this policy does not reflect practice, or if concerns are not acted upon promptly.

All pupils

- The boundaries of use of ICT equipment and services in this school are given in the pupil Acceptable Use Policy (Annex A); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- e-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

- Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, the website, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.
- Parents must also understand the school's need to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Adelaide Primary School uses a range of devices including PCs, Laptops, iPads and Chromebooks. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

- Internet Filtering – we use a Smoothwall Filter managed by our Internet Service Provider that prevents unauthorized access to inappropriate online content. Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy, or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher

and IT support. If staff or pupils discover unsuitable sites, the URL and content must be reported to the E-Safety lead and IT Support and appropriate measures will be taken to ensure safety.

- Filtering and monitoring systems are reviewed regularly and formally evaluated at least once every academic year by the member of the Senior Leadership Team responsible for filtering and monitoring, with support from the Designated Safeguarding Lead and IT Support. Records of the review will be retained.
- Encryption – All school devices that hold personal data (as defined by UK GDPR and the Data Protection Act 2018) must be encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
- Passwords – all staff and pupils will be unable to access any device without a unique username and password, except for classroom iPad's that are used under staff supervision. Staff and pupil passwords will change on a regular basis or if there has been a compromise, whichever is sooner. IT Support will be responsible for ensuring that passwords are changed.
- Anti-Virus – All capable devices will have anti-virus software. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. IT Support will continue to monitor and update anti-virus software.

Safe Use

- Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.
- Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.
- Mobile Phones – Adelaide Primary School operates as a mobile-phone-free environment during the school day. Pupils bringing mobile phones to school must hand them into the school office on arrival and collect them at the end of the school day. Pupils must not have access to mobile phones during lessons, transitions, breaktimes or lunchtimes unless exceptional circumstances have been agreed by the Headteacher.

- Photos and videos – Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

- Social Media and Online Platforms –Adelaide Primary School uses a range of approved online platforms, applications and digital services to support teaching and learning, assessment, safeguarding, curriculum delivery , staff development and communication with parents and carers.
- Teaching and Learning Platforms – Pupils may access approved educational platforms to support learning across the curriculum, including reading, writing, mathematics and computing. Access is controlled through secure usernames and passwords and pupil activity is overseen by school staff.
- School Systems and Professional Platforms – Staff may access approved management, safeguarding, assessment, curriculum and communication platforms to support the effective operation of the school.

Access is restricted to authorised users and managed in accordance with the school's data protection, safeguarding and acceptable use procedures.

- Home-School Communication – The school uses approved communication platforms, including Arbor, Class Dojo and Facebook, to communicate with parents and carers and share information relating to pupils' learning, behaviour and achievements.

- In addition, the following is to be strictly adhered to:
    - Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
    - There is to be no identification of pupil using first name and surname; first name only is to be used.
    - Where services are "comment enabled", comments are to be set to "moderated".
    - All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

- Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day after notification.

Incidents

It is vital that all staff recognise that e-Safety is a part of safeguarding. The Trust commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of the Trust and the LADO (Local Authority's Designated Officer). The school will actively seek support from other agencies as needed (i.e. the local authority - Children's Social Care, National Crime Agency, CEOP, Police, IWF).

Online safety incidents may include concerns relating to Artificial Intelligence (AI), including AI-generated images, deepfakes, synthetic media, impersonation, algorithmic manipulation, AI-enabled grooming, AI-assisted bullying, harassment, sexualised content and identity misuse. Such concerns will be managed through the school's safeguarding and child protection procedures. We will inform parents/carers of e-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in their absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum

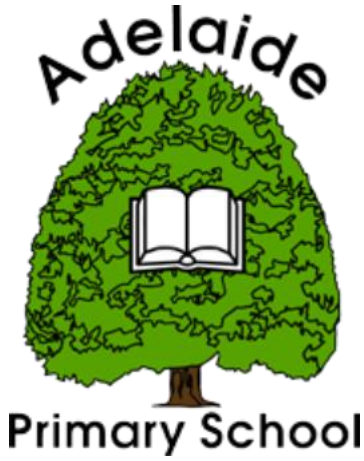
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Adelaide Primary School will have an annual programme of training which is suitable to the audience.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. E-safety messages are constantly revisited e.g. participating in national e-safety week, ICT & PSHE curriculum etc.

Online safety education will include emerging technologies such as Artificial Intelligence (AI). Pupils will be taught how to use AI safely and responsibly, how to identify misinformation and AI-generated content, and how to report concerns. Staff training will include awareness of safeguarding risks associated with AI, including deepfakes, synthetic media, AI-enabled grooming, bullying, harassment and reputational harm.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

Annex A



Acceptable Use Policy – Pupil Charter of Good Online Behaviour
Year 5 & Year 6

- I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.
- I will not – deliberately look for or show other people anything that could be upsetting.
- I will not – deliberately look for, or access inappropriate websites or apps. I will consider the age-appropriate certificate when playing games or viewing videos.
- I Promise – to show respect for the work that other people have done.
- I will not – use other people's work or pictures without permission to do so.
- I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.
- I will not – share my password with anybody. If I forget my password, I will let my teacher know.
- I will not – use other people's usernames or passwords.
- I will not – share personal information online with anyone.
- I will not – get involved in incidents of cyber-bullying either at school or home via apps or websites such as Twitter, Facebook, Instagram (social media) WhatsApp, Discord (Messaging apps)
- I will not – download anything from the Internet unless my teacher has asked me to.
- I will – let my teacher know if anybody asks me for personal information.
- I will – tell my teacher immediately if I find anything inappropriate.

  I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

  I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.
- I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
- I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Pupil): Date :

Primary School

Acceptable Use Policy – Pupil Charter of Good Online Behaviour
Year 3 & Year 4

- I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do
- I will not – look for or show other people anything that could be upsetting
- I will not – use other people's work or pictures
- I will not – share my password with anybody. If I forget my password, I will let my teacher know.
- I will not – use other people's usernames or passwords.
- I will not – share personal information online with anyone.
- I will not – share nasty messages online (cyber-bullying) either at school or home
- I will not – download anything from the Internet unless my teacher has asked me to
- I will – let my teacher know if anybody asks me for personal information
- I will – tell my teacher straight away if I find anything upsetting
- I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
- I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.
- I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Pupil) : Date :

Annex C Risk Log

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	e-Safety Officer IT Support
2.	Blogging	Inappropriate comments	2	1	2	e-Safety Officer IT Support
2.	Blogging	Using copyright material	2	2	4	e-Safety Officer IT Support
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	e-Safety Officer IT Support

Likelihood: How likely is it that the risk could happen (foreseeability).
Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)
Likelihood and Impact are between 1 and 3, 1 being the lowest. Multiply Likelihood and Impact to achieve score.
LEGEND/SCORE:
1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body. Final decision rests with Headteacher and Governing Body

Annex D Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school- owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
Likelihood **3**	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact **3**	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
RISK ASSESSMENT	**HIGH (9)**
Risk Owner	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school.

	Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Approved	
Date	**Sept 26**
Signed (DSL)	**M Anthony**
Signed (Safeguarding Governor)	