E-Safety Policy

(Including the use of personal devices, and social media)

Unity
Trust
Courage
Curiosity
Respect
Kindness

A community for learning. Raising expectations. Fulfilling high standards.

This Policy was revised: **January 2024**
The policy is to be reviewed: **January 2025**
Headteacher: **Mrs Gemma Hillier**

Contents

1. Introduction
2. Scope
3. Links to other policies and national guidance
4. Aims and Objectives
5. Roles & Responsibilities
6. Managing ICT Systems and Access
7. E-Mail/Communication
8. Personal Devices
9. Use of Social Media
10. Responses to Incident of Concern

1. Introduction

New technologies inspire children to be creative, communicate and learn, and, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Widmer End Community Combined School endeavours to highlight both the benefits and risks of using technology and aims to provide a robust education for users to enable them to control their online experience.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Positive Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

3. Links to other policies and national guidance

The following school policies and procedures should also be referred to:

- Child Protection Policy
- Whistleblowing policy
- Positive Behaviour Policy
- Anti-Bullying Policy
- Staff code of conduct
- Data Protection Policy

The following local/national guidance should also be read in conjunction with this policy:

- Keeping Children Safe in Education 2023
- Teaching Online Safety In Schools 2024
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.
- PREVENT Strategy HM Government

4. Aims and Objectives

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well. It is our belief that we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.
Through our PSHE programme of Study (Jigsaw) and our Computing Curriculum, alongside day-to-day school life, we will:

- Provide opportunities throughout our curriculum for E-Safety to be taught.
- Discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons and whole school activities; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Ensure that any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Teach pupils how to use a range of age-appropriate online tools in a safe and effective way.
- Remind pupils about their responsibilities through their lessons and through our school's core values.
- Model safe and responsible behaviour in their own use of technology during lessons.
- Teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, guide pupils to use age-appropriate search engines (all use will be monitored and pupils will be reminded of what to do if they come across unsuitable content).
- Teach pupils about the impact of online bullying and know how to seek help if they are affected by any form of online bullying (see Anti-Bullying Policy).
- Make pupils aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as

Childline or the CEOP report abuse button.

5. Roles and Responsibilities

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed
- in the event of a serious online safety allegation being made against a member of staff. (see later section – "responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

ICT support

The school outsources its ICT support. In partnership with the headteacher, ICT support ensures that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any Local Authority / Academy Group / other relevant body Online Safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- appropriate filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of school internet-enabled activity is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher for investigation

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school / academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or a Senior member of staff
- all digital communications with pupils and parents/carers should be on a professional level and only

carried out using official school systems

- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the taught principles of how to be safe online.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

- are responsible for using the school technology systems in accordance with the taught principles of online safety
- Must only use their own personal 'log in' or account details when using school technology
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, where age-appropriate
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know how to respond to any concerns or worries they have
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, the school website and information about national and online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- communication and social media (also see anti-bullying & positive behaviour policies)
- access to parents' sections of the website and on-line pupil records

6. Managing ICT Systems and Access

The school believes that the most effective method to ensure our pupils' safety online is to teach them safe behaviours. However, the school does consider the hardware and software used to ensure layers of protection.

- Users will be made aware that they must take responsibility for their use and behaviour when using the school ICT system and that such activity will be monitored and checked.
- While in school, pupils will access the network on school devices only.
- The network is secured and appropriate filtering is in place. The school adopts a filtering system that aligns with industry standard best practice.
- Where appropriate, some children will have an individual user account with an appropriate password which will be kept secure.
- All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the school's network using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password.
- Temporary members of staff (e.g. Supply teachers) are given a temporary log-in with limited access to the school's data and information.

7. E-Mail/Communication

- Staff should only use approved accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked. Communication with parents should only be in the form of an email through Arbor or school account, through Dojo or by phone call.
- Staff should not use personal email accounts or social media for professional purposes, especially to exchange any school related information or documents or to email parents/carers or other professionals. (see also Social Media section below)
- Staff should not send emails to pupils.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive messages.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.

8. Personal Devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or school time, unless otherwise agreed with the Headteacher. They should be switched off or silent at all times. Mobile devices can only be used during break and lunchtimes and are restricted to being used in the staff room or PPA area
- No images or videos will be taken on mobile phones or personally owned devices.
- In the case of school productions, when parents/carers are permitted to take pictures of their child in accordance with school protocols, such photographs are deemed for personal use and, therefore, should not be posted online or shared beyond personal use.
- The sending of abusive or inappropriate text, picture or video message is forbidden.
- Laptops and/or other devices provided by the school are for work-related use only.
- Pupils should not bring internet-enabled devices to school. Any requests for such items should be discussed with the Headteacher.

9. Use of Social Media

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school. Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
The tone of content published on social media should be appropriate to the audience, whilst retaining

appropriate levels of professional standards. Key words to consider when composing messages are:

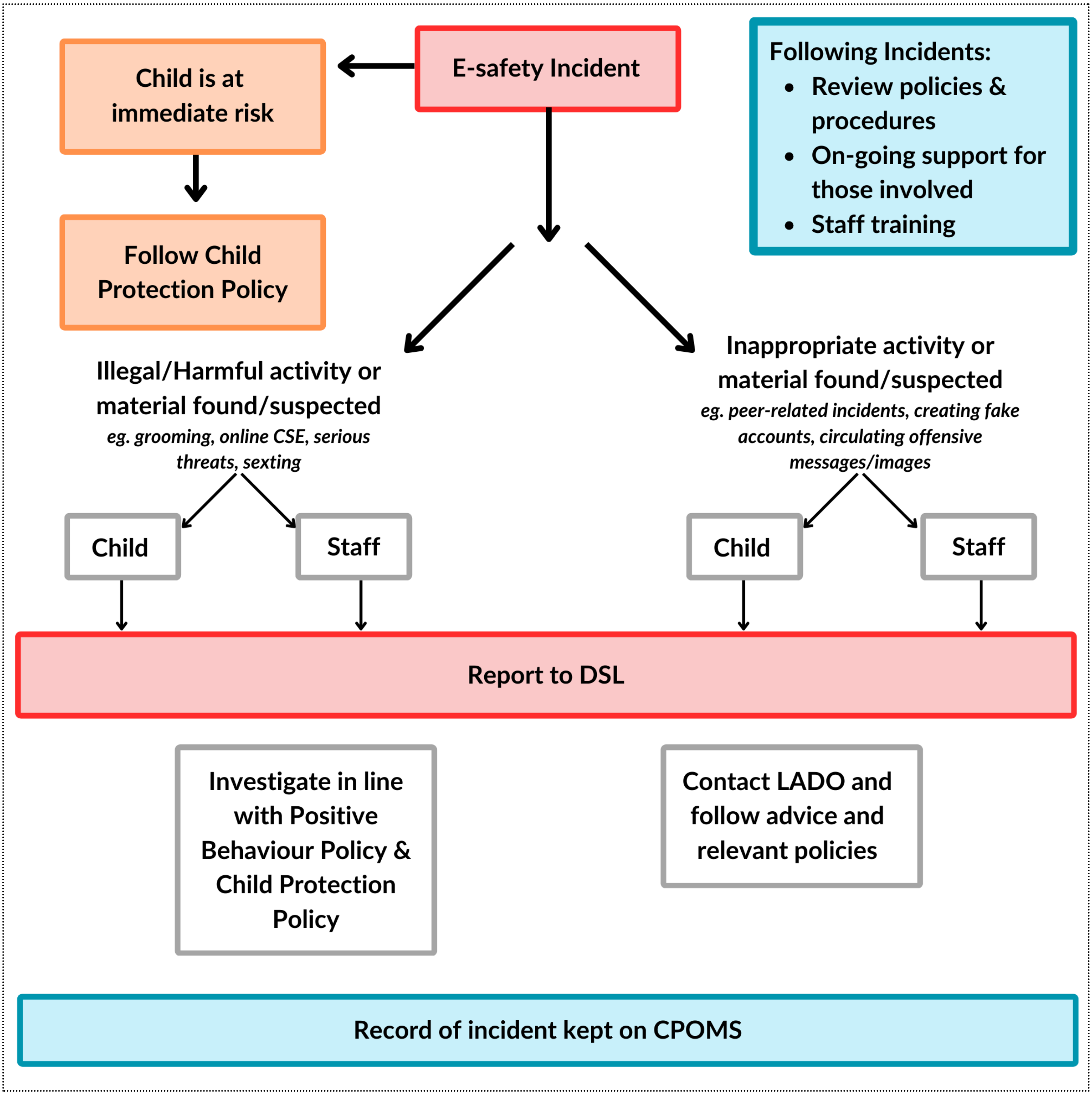
- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Permission to use any photos or video recordings should be sought in line with the school's data protection policy. Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts. Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts.

10. Responses to Incident of Concern

Any incidents of concerns will be dealt with in line with the school's Positive Behaviour policy or Child Protection policy and a record kept on CPOMS.

Misuse of the internet or devices may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.



E-safety Incident

Child is at immediate risk

Follow Child Protection Policy

Following Incidents:

- Review policies & procedures
- On-going support for those involved
- Staff training

Illegal/Harmful activity or material found/suspected

eg. grooming, online CSE, serious threats, sexting

Inappropriate activity or material found/suspected

eg. peer-related incidents, creating fake accounts, circulating offensive messages/images

Child

Staff

Child

Staff

Report to DSL

Investigate in line with Positive Behaviour Policy & Child Protection Policy

Contact LADO and follow advice and relevant policies

Record of incident kept on CPOMS