MENGHAM JUNIOR SCHOOL

e-safety Policy

Palmerston Road,
Hayling Island,
Hants.
PO11 9ET

Tel: 023 92462162

E-mail: adminoffice@mengham-jun.hants.sch.uk

Ratified by Governors: January 2026

Review: annually

Review Date: January 2027

Table of Contents

Introduction & Ethos

The school e-safety Policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The E-safety Policy encourages appropriate and safe conduct and behaviour when achieving this. It is underpinned by the school's Acceptable Use of ICT Policy.

The school will make reasonable use of relevant legislation and guidelines to inform positive behaviour regarding ICT and Internet usage both on and off the school site. This will include imposing sanctions for inappropriate behaviour in line with the regulation of student behaviour under the Education and Inspections Act 2006.

Pupils, staff and all other users of school-related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. It is intended that the positive effects of the policy will be seen online and offline, in school and at home and, ultimately, beyond school and into the workplace.

The E-safety Policy and Acceptable Use of ICT Policy will be reviewed at, or prior to, the start of each academic year and promptly in the following instances:

- Serious and/or frequent breaches of the Acceptable Internet Use of ICT Policy or in the light of e-safety incidents.
- New guidance by government/local authority/safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- e-safety incidents in the community or local schools which might impact on the school community.
- Advice from the police and/or local safeguarding children partners.

Who this policy applies to:

The school E-safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related Internet, computer systems and mobile technologies internally and externally.

'In loco parentis' provision under the Children Act 1989 also allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils and removing inappropriate content.

Scope

This e-safety policy covers the use of:

- School-based ICT systems and equipment
- School-based Intranet and networking
- School-related external Internet, including but not exclusively, extranet, e-learning platforms, blogs and social media websites
- External access to internal school networking, such as webmail, network access, file-serving (document folders) and printing
- School ICT equipment off-site, for example, staff laptops, mobile phones and tablets
- Pupil and staff personal ICT equipment when used in school and which makes use of school networking, file-serving or Internet facilities
- Tablets, mobile phones, devices and laptops when used on the school site

Roles & Responsibilities

Headteacher (also Digital Lead)

The headteacher is responsible for:

- Determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors.

- Agreeing criteria for the acceptable use by pupils, school staff and governors of Internet capable equipment for school-related purposes or in situations which will impact on the reputation of the school, and/or on school premises.

They will ensure that:

- There is a cycle of evaluation and review based on new initiatives and partnership discussion with stakeholders and outside organisations, technological and Internet developments, current government guidance and school-related e-safety incidents.
- Good practice is implemented within the teaching curriculum and wider pastoral curriculum.
- Training development is identified and provided for staff and governors and guidance provided to parents, pupils and local partnerships.

Computing Lead / e-safety officer

The school has a designated computing lead who coordinates e-safety provision across the school and wider school community.

The e-safety coordinator is responsible for e-safety issues on a day-to-day basis including:

- Auditing and assessing requirements for staff, support staff and governor e-safety training, and ensuring that all staff are aware of their responsibilities and the school's e-safety procedures.
- Promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents and partner stakeholders.
- Along with IT support (Agile), risk assessing new technologies, services or software.

The school's finance officer
The school's finance officer is responsible for is responsible for Liaising with LA contacts and the school ICT support (Agile ICT).

They will also receive and distribute reports to the headteacher on internet usage provided by Agile ICT.

Governors
The school has appointed Claire Edwards as having responsibility for e-safety.

This governor will:

- Review this policy 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.
- Receive regular updates from the Headteacher or E-safety officer/Computing lead in regards to training, identified risks and any incidents.

ICT support staff & external contractors (Agile ICT)

Internal ICT support staff and technicians are responsible for:

- Maintaining the school's networking, IT infrastructure and hardware.
- Keeping up to date with current thinking and trends in IT security.
- Ensuring that the school system, particularly file-sharing and access to the Internet, is secure.
- Taking all reasonable steps to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- Maintaining and enforcing the school's password policy and monitoring and maintaining the Internet filtering.
- Ensuring external contractors, such as VLE providers, website designers/hosts/maintenance contractors, are made aware of, and comply with, the school's e-safety policy.

- Completing DBS checks where contractors have access to sensitive school information and material covered by the Data Protection Act.

Where IT is outsourced, for example connectivity, maintenance, cloud-based services, website and email provision, filtering and anti-virus, the school needs to ensure that they comply with DfE guidance and that a Service Level Agreement (SLA) is in place to provide school standard provision and support.

Teaching and teaching support staff

Teaching and teaching support staff need to:

- Ensure that they are aware of the current school policy, practices and associated procedures for reporting e-safety incidents.
- Read, understand and sign the Acceptable Use Policies relevant to Internet and computer use in school.
- Rigorously monitor pupil Internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the school site.
- Promote best practice regarding avoiding copyright infringement and plagiarism.
- Be aware of online propaganda and help pupils with critical evaluation of online materials.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.
- Report any concerns to the e-safety officer and headteacher.

Designated Safeguarding Lead (DSL)

Odele Davies is the school's Designated Safeguarding Lead. The DSL is trained in specific e-safety issues to enable them to decide which e-safety incidents are required to be reported to CEOP, local Police, LADO, local safeguarding partners, Trust CEO, social services and parents/guardians; and also to determine whether the information from such an incident should be restricted to nominated members of the leadership team.

The DSL acts 'in loco parentis' and will liaise with websites and social media platforms if required such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

Pupils

Pupils are required to:

- Use school Internet and computer systems in agreement with the terms specified in the school Acceptable Use Policies.
- Understand that the policies also cover the use of personal items such as phones and their internet use out of school on social networking sites such as

Instagram if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation, or illegal activities.
- Be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.

Parents & carers

Parents and carers are asked to support the school's stance on promoting good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

The school expects parents and guardians to sign the school's Acceptable Use Policies, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums, social media, online reporting arrangement, questionnaires and the VLE.

The school will provide opportunities to educate parents on e-safety.

Other users

School visitors, wider school community stakeholders and external contractors should be expected to agree to a visitor's AUP document or a tailored AUP document specific to their level of access and usage.

External users with significant access to school systems which include sensitive information or information held securely under the General Data Protection Regulations should be DBS checked. This includes external contractors who might maintain the school domain name and web hosting – which would facilitate access to cloud file storage, website documents and email.

e-safety in Practice

The school will ensure that:
- School computer systems are fit for purpose and customised to ensure e-safety while meeting teaching and learning requirements.
- It is possible to trace every login, data transaction, or other activity to a particular user on laptops.
- Servers, network switches, cloud-based systems, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.
- Regular audits of systems are carried out.
- The school's Internet service is provided by a fully accredited ISP.
- Filtering and monitoring is in place and any filtering incidents are examined to prevent a reoccurrence.
- Children have passwords to access software.
- The school has protocols in place to meet the requirements of GDPR as defined by the Information Commissioner's Office.

- When disposing of equipment, the school ensures all data is wiped irretrievably.
- Policies are in place around the taking and sharing of images of children.
- The school will make it clear to pupils and staff which online and network activities are appropriate and which are not.

E-safety Education Programme

The school's e-safety education is delivered through:

Pupils

- Project Evolve resources at the start of every computing unit
- e-safety as part of pastoral care –assemblies.
- e-safety events –Safer Internet Day.
- Pupils are asked to sign an acceptable use of ICT contract when their child is admitted to the school. This is sent out annually.
-

Parents and wider school community

- E-safety information directly delivered to parents: letters, newsletters or the school's website.
- Parents' evenings, open days, transition evenings, or other events to take advantage of occasions when there are large numbers of parents in school.
- Parents are asked to sign an acceptable use of ICT contract when their child is admitted to the school. This is sent out annually.

Staff

- Online training directly delivered to staff at least annually.
- The e-safety policy will be updated and evaluated by staff annually.
- The e-safety coordinator should be the first port of call for staff requiring e-safety advice.
- The Acceptable Use of ICT Policy is reviewed annually. Staff sign to say they have read this annually.

Governors

- e-safety information directly delivered to governors: letters, newsletters, school website or Governor Hub.
- Open days, or other events to take advantage of occasions when there are large numbers of visitors in school.
- Governors should also be provided access to staff inset training, or specific governor training provided externally (for example through Hampshire governor training courses).

ICT support staff (Agile)

- IT support staff and contractors should ensure that bought in hardware and software solutions feature built in training provision.
- Support staff and contractors need to be DBS checked.
- IT technical support staff and network managers should have relevant industry experience and Microsoft/Cisco certified qualifications.

Key Messages of the Education Programme

Particular behaviour which will be highlighted might include:

- Explaining why harmful or abusive images on the Internet might be inappropriate or illegal.
- Explaining why accessing age inappropriate or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
- Explaining how accessing and/or sharing other people's personal information or photographs might be inappropriate or illegal.
- Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
- Exploring how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
- Teaching pupils to assess the quality of information retrieved from the Internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- Encouraging responsible and effective digital literacy skills;
- The medical and social effects of spending too much time on the Internet, games consoles or computers.

Dealing with e-safety Incidents

Typical e-safety incidents perpetrated by pupils, staff, parents, governors, contractors and others include:

- Finding illegal material on the network which could raise a child protection issue.
- Going on the Internet during lesson time for reasons not related to the lesson.
- Bypassing the school's filtering system.
- Viewing pornographic material.
- Using a mobile phone or other digital device in a lesson.
- Using social media or email during a lesson.
- Cyber bullying.
- Writing malicious comments about the school or bringing the school name into disrepute (whether in school time or not).
- Sharing usernames and passwords.
- Deleting someone else's work or unauthorised deletion of school files.
- Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud using the school network.
- Uploading or downloading files using the school network.
- Copyright infringement of text, software or media.
- The school's approach to dealing with an incident and applying sanctions aims to demonstrate the correlation between procedures and sanctions for pupils and procedures and sanctions for staff.

The reporting process and sanctions will depend on:

- Whether an illegal act has taken place
- Whether there is a safeguarding issue (in which case we will follow the guidelines in our Safeguarding Policy)
- The nature and severity of the incident
- Whether the person has previously had sanctions for a similar incident

Note that under The Education and Inspections Act 2006 headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.

These general principles apply in dealing with an incident:

- Evidence should be collected and preserved – this may involve assistance from the school network manager, IT support or external IT contractor.
- Incident reports will be completed by Odele Davies.
- Appropriate disciplinary action/sanctions will be taken following the school's procedures.
- Parents/carers may be informed.
- The police and/or other relevant agencies will be notified in certain circumstances, including:
    - if an indecent image has been taken
    - in the case of cyber bullying
    - An incident of hacking or online fraud

- Offending content will be removed if possible.
- A review of security will be carried out where relevant.

Useful links

Ofsted:
www.gov.uk/government/publications/school-inspection-handbook-eif
DfE:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools
The Think u Know website by Child Exploitation and Online Protection (CEOP) Website:
www.thinkuknow.co.uk/parents or www.thinkuknow.co.uk/teachers
CEOP:
www.ceop.police.uk/safety-centre/
Childnet:
http://www.childnet.com/
UK Safer Internet Centre:
www.saferInternet.org.uk/safer-Internet-day
www.saferInternet.org.uk/
Internet Watch Foundation:
www.iwf.org.uk
www.iwf.org.uk/members/get-involved

Links to training:
E-safety Support: online refresher training www.e-safetysupport.com/online_training

Movies and presentations:
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware

Other publications:

- Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/byronreview/.
- Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/.