Technology and E-Safety Policy

Responsibility of JJM
Reviewed: September 2023 and to be reviewed October 2024

Responsibilities

The Senior Management Team (SMT) member responsible for e-safety - Jo MacLelland
The e-safety coordinator - Tom Vivian (Head of IT)

It is also a key role of the Designated Safeguarding Lead (DSL) to ensure the teaching and education of online safety.

The e-Safety coordinator is responsible for delivering staff development and training, recording incidents, reporting any developments, monitoring and reporting incidents of cyberbullying and liaising with the Governors and external agencies to promote e-safety at Aysgarth School. He may also be required to deliver workshops for parents.

This policy applies to staff and pupils in the Prep and Pre-Prep including EYFS.

This policy in relation to cyberbullying works alongside the Anti Bullying Strategy.

This policy is in relation to the Aysgarth School - ICT Strategy, Internet use and Acceptable Use Policies (AUPs)

Aysgarth School has a clear policy about access to and the use of the Internet. Please refer to the “Internet Safety and Acceptable Usage Policy” for further guidance.

All pupils, parents and staff will sign an Acceptable Use Policy (AUP)

The pupil's and parents' AUPs can be found in the Parents Handbook and A Guide to Boarding. The staff AUP can be found in the Code of Conduct.

An email will be sent to parents of all new boys asking them to digitally sign acceptance of the AUP.

All AUPs will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group, at the start of every year.

AUPs will be given to pupils and parents in their native language, where possible.

Under no circumstances should staff access inappropriate images. It may be that the Head of IT and Deputy Head may need to access inappropriate material during an investigation. The Headmaster will be informed of this process.

Accessing child pornography or indecent images of children on the Internet, and making, storing or disseminating such material, is illegal and, if proven, will invariably lead to the individual being barred from working with children and young people.

Using school equipment to access inappropriate or indecent material, including adult pornography, would normally lead to disciplinary action, particularly if as a result pupils might be exposed to inappropriate or indecent material.

Technical Provision & Safeguards

Technical Provision

The Head of IT is employed to oversee the maintenance & running of the school's IT system. All teachers have laptops; there is 1 IT suite in the Prep School; all the Pre Prep and Prep pupils have access to Chromebooks. The Pre Prep has a set of 16 iPads; the Boarding Department has 6 Chromebooks
There are 3 main servers that manage network services and resources. They are backed up every day and backups are stored offsite.

There is a physical network running gigabit to the network points and a wireless network that covers 90% of the school site. Staff laptops log on to a secure hidden SSID and the Chromebooks log on to a different hidden SSID. There is also provision for guest access to wifi which does not allow access to network resources, only the internet. The guest's SSID password is changed regularly.

Safeguards

Filtering Systems

As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, Aysgarth ensures that appropriate filters and appropriate monitoring systems are in place and staff have been trained on their responsibility in accordance to managing and using the filters.

Internet security and content filtering is managed by a Fortigate Firewall. The firewall is a NGFW (Next Generation Firewall). We use 2 separate policies for staff members' and pupils' access to websites.

All outgoing pupil emails are filtered by Google. Should unsuitable language be detected then the email is copied to the e-safety coordinator & Deputy Head who act accordingly.

If a pupil or member of staff tries to access an unsuitable website this will be logged by Fortinet. The e-safety coordinator has the ability to check this list regularly. A weekly report is sent to the e-safety coordinator. When required, the e-safety coordinator is able to conduct a more thorough check of the use of the internet.

Staff laptops and IT lab computers have Sophos antivirus software installed which also uses content filtering polices and ransomware detection.

All staff are trained to understand the importance of being aware that filter systems can fail and allow access to a possibly inappriopriate site. Staff must be aware of these problems and must report them to their line manager and e-safety coordinator.

Use of Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. Many school activities involve recording images. These may be undertaken as part of the curriculum, as out-of-school activities, for publicity, or to celebrate achievement. However, it is important that consent from all parents (especially of EYFS children) is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then the names of pupils should not be linked to them.

Using images of children for the school's publicity purposes has already had the consent of parents through the Parental Contract. Staff are fully aware of any children whose parents have requested that their image is not used when considering the use of images. All staff will be informed of any child that should not be photographed or videoed during the most relevant staff meeting, which is minuted.

Staff need to be aware of the potential for these aspects of teaching to be misused for radicalisation, pornographic or 'grooming' purposes. Careful consideration should be given as to how these activities are organised and undertaken.

Staff may **not** use their own device to capture images. A school camera or device should be used to capture images. Photos taken by the school are subject to the Data Protection Act. All photos taken on devices should be transferred to the school server or uploaded to the school website, Twitter or Facebook accounts. No images should be retained on any personal device unless they are in the public domain. Images should not be displayed on other websites, in publications or in a public place without additional consent.

Online (remote teaching) lessons should be conducted using Google Meet. The lessons must be recorded and linked directly to the calendar entry for viewing at a future date. One-to-one lessons should include an invitation for a line manager to attend the session.

This means that staff should:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded
- ensure that a senior member of staff is aware that the school photography/image equipment is being used and for what purpose.
- ensure that all images are available for scrutiny in order to screen for acceptability
- avoid taking images in one-to-one situations
- record online lessons, using Google Meet, and invite a line manager to the session if it is a one-to-one situation.

This means that staff should not:

- use personal devices to capture images of pupils.
- have images of pupils stored on personal cameras, devices or home computers.
- make images of pupils available on the Internet, other than through the school network/websites without permission from parents and senior staff.

Mobile phones and other devices

All staff mobile phones should be switched to silent whilst on the school premises, and should not be used in the presence of the pupils. (Except in an emergency). Mobile phones

are not permitted in the EYFS or in any area where EYFS children are present. Only school devices should be used to capture photographs and videos. School mobiles are made available to staff for school use only.

There should be no pupil SIM cards in school. All overseas pupils' SIM cards must be handed to the Deputy Headmaster. If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated, but staff should not 'search' the phone. The phone should be given to the Deputy Headmaster who will deal with the matter in line with normal school procedures.

Use of emails

Pupils should only use their email address that has been issued by the school. Staff members are given an @aysgarthschool.co.uk email account which is a work email account, and as such will be used predominantly for professional purposes.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the device if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a computer to be 'locked').

Data storage

Staff should not store sensitive data on a USB device or laptop. Under no circumstances should the school database (SchoolBase) be copied onto a laptop or USB device. Staff need to risk assess any data that they plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact.

E-Safety education

E-safety is taught throughout each year group in the prep school. In each year group, we dedicate up to 2 whole lessons on e-safety. Within the ICT scheme of work, there is built-in a clear e-safety outcome that runs through the subject content. For more information please see the ICT schemes of work.

We also have a program of online training and refresher courses for the staff as well as various fact sheets and online training for parents. We periodically get outside speakers to talk to the whole school, staff and parents about e-safety.

Parents and governors are regularly updated with information about the e-safety processes and the curriculum. They are also given access to additional information and suitable websites by the Head of IT. (see table below)

Pupils	
Forms 1 & 2	Staying Safe on the Internet
Forms 3-5	Online Communication - The Good, The Bad and The Dangerous Danger in the Age of Online Communication Online Fact, Fiction and Myth
Staff	
	E-safety for Teachers - Annual Training Social Media for Teachers - Annual Refresher
Parents & Governors	
	Audit survey - Questions for Parents/Guardians E-safety Factsheets for Parents & Governors E-safety for Parents online course - https://nationalonlinesafety.com/courses/online-safety-klass-for-parents-and-carers-ages-7-11 https://info.nationalonlinesafety.com/free-parents-course

Reporting

All breaches of the e-safety policy need to be recorded via the E-safety incident form which will be managed by the Head of IT. The details of the user, date and incident should be reported. Incidents of cyberbullying, or incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action. All staff should be aware of the school's child protection procedures, including procedures for dealing with allegations against staff.

- Please see the Safeguarding Policy, which can be found on the School's website. Incidents that are not child protection issues but may require SMT intervention should be reported to SMT immediately. Allegations involving staff should be reported to the Headmaster. If the allegation is one of abuse then it should be

handled according to the Aysgarth Code of Conduct - Sharing Concerns and Recording Incidents (Safeguarding Policy). The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline etc.)

Infringements and sanctions

Whenever a pupil or staff member infringes the Technology and E-Safety Policy, the final decision on the level of the sanction will be at the discretion of the senior management team. The following are provided as examples only:

1) Pupils
    a) Level 1 Infringement
    Use of non-educational sites during lessons; Unauthorised use of email; or Unauthorised use of a mobile phone (or other new technologies)
    [Possible Sanctions: minus or penalty / referred to form tutor / Head of IT/ confiscation of device removal of IT room access during free-time]
    b) Level 2 Infringements
    Continued use of non-educational sites during lessons after being warned; Continued unauthorised use of email after being warned; Use of unauthorised instant messaging/social networking sites; Accidentally corrupting or destroying others' data without notifying a member of staff of it, or Accidentally accessing offensive material and not notifying a member of staff of it.
    [Possible Sanctions: detention / referred to Form Tutor or e-safety Coordinator/removal of IT room access during free time/removal of Internet access rights for a period / Chromebook stored with Head of IT / additional entry in Day Book (SchoolBase)]
    c) Level 3 Infringements
    Deliberately corrupting or destroying someone's data, violating the privacy of others; Sending an email or message that is regarded as harassment or of a bullying nature (one-off), or Deliberately trying to access offensive or pornographic material.
    [Possible Sanctions: referred to Form Tutor / e-safety Coordinator / removal of IT room access during free-time / Deputy Headmaster / removal of Internet rights for a period / contact with parents]
    Other safeguarding actions if inappropriate web material is accessed:
        i) Ensure additional and appropriate technical support filters the breached site - this would be organised by the Head of IT
    d) Level 4 Infringements
    Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned; Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist,

homophobic or violent; Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998; or Bringing the school name into disrepute.
[Possible Sanctions – Referred to Headmaster / Contact with parents / possible exclusion / refer to Community Police Officer]
Other safeguarding actions:

i) Secure and preserve any evidence.
ii) Inform the sender's email service provider if a system other than the school system is used. Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

2) Staff

a) Level 1 Infringements (Misconduct)
Excessive use of the Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc; Misuse of first-level data security, e.g. wrongful use of passwords; Breaching copyright or licence e.g. installing unlicensed software on the network; or Not locking the computer when leaving the room.
[Sanction - Head of IT. Warning given.]

b) Level 2 Infringements (Gross Misconduct)
Serious misuse of, or deliberate damage to, any school computer hardware or software; Any deliberate attempt to breach data protection or computer security rules; Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998; or Bringing the school name into disrepute.
[Sanction – Referred to Headmaster / Governors and follow school disciplinary procedures, report to Police.]