Aylesford School
and Sixth Form College

wonder aspiration respect discipline

E-Safety Policy

Written/Updated:	May 2019
Review date:	May 2020
Lead:	Assistant Headteacher (Safeguarding)
Via:	Standards, Personnel and Curriculum

'from potential to reality'

Tapping Way, Warwick, Warwickshire, CV34 6XR
Tel: 01926 747100 **Fax:** 01926 494194 **Email:** office@aylesford-elearning.net **Web:** www.aylesfordschool.org.uk
A charitable company registered in England and Wales, company number 7848367
Headteacher: Steven Hall BSc MA

Contents

Scope of the Policy
This policy applies to all members of the *Aylesford School* community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of ICT systems, both in and out of the *school*. The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of students when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-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. The *school* will deal with any such incidents in compliance with the behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors Safeguarding Sub Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governors Safeguarding Sub Committee* has taken on the role of *E-Safety Governor*. The role of the E-Safety *Governor* will include:

- *termly meetings with the DSL and head of ICT*
- *monitoring of e-safety incident logs*
- *reporting to relevant Governors / committee*

Headteacher
The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead (DSL), Head of ICT, and the Senior ICT Technicians. In the event of a serious e-safety allegation being made against a member of staff, the Headteacher will comply with protocols outlined in the appropriate disciplinary policies. The Headteacher is responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Deputy Headteacher with responsibility for ICT, Senior ICT Technicians/Technical staff

Technical – infrastructure/equipment, filtering and monitoring

It is the responsibility of the Deputy Headteacher with responsibility for ICT, in liaison with the Senior ICT Technician to ensure that the managed service provider carries out all appropriate e-safety measures. They will ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this. Policy are implemented. The Deputy Headteacher responsible ICT, Senior ICT technicians/Technical Staff are responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack: specifically -

1 *that users may only access the networks and devices through a properly enforced password protection policy (eg the active directory and WiFi)*
2 *that filtering systems are applied and updated on a regular basis and that their implementation is not the sole responsibility of any single person.(eg Smoothwall, Syscomm webfilter)*
3 *that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant*

4 *that the use of the network / internet / Virtual Learning Environment / remote access / and staff and student accounts is regularly monitored (through the use of trackers, clean-ups, liaison with staff) in order that any misuse / attempted misuse can be reported to the Headteacher, DSL or other relevant colleague for investigation/action/sanction.*

5 *There will be regular reviews and audits of the safety and security of school technical systems*

6 *Servers, wireless systems and cabling must be securely located and physical access restricted*

7 *All users will have clearly defined access rights to school technical systems and devices through 'security groups'.*

8 *All users (at KS2 and above) will be provided with a username and secure password by the Senior ICT Technicians who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. (Aylesford Primary School may, if required, choose to use group or class log-ons and passwords for KS1 and below)*

9 *The "administrator" passwords for the school ICT system, used by the Senior ICT Technician (or other person) must also be available to the Headteacher and Deputy Headteacher and kept in a secure place (eg the school safe)*

10 *The Senior ICT Technicians are responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations*

11 *Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear, audited process in place to deal with requests for filtering changes (eg Smoothwall, Syscomm webfilter).*

12 *The Senior ICT Technicians will provide differentiated user-level filtering (allowing different filtering levels for different groups of users – SLT/staff/students/ etc)*

13 *The Senior ICT Technicians /technical staff regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*

14 *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person*

15 *Appropriate security measures are in place (Sophos) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested annually and 'live monitored'. The school infrastructure and individual workstations are protected by up to date antivirus software.*

16 *An agreed protocol is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.*

17 *An agreed protocol is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*

Bring Your Own Device (BYOD) (*Post-16 Students Only)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be addressed. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

Designated Safeguarding Lead (DSL)

- *take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety protocols*
- *ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place*
- *provides training and advice for staff*
- *liaises with the Local Authority/relevant body*
- *liaises with school technical staff*
- *receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments*
- *meets termly with the Governors Safeguarding Sub Committee to discuss current issues, review incident logs and filtering*
- *reports regularly to Senior Leadership Team*

The Head of ICT

The Head of ICT will be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:-

- *sharing of personal data*
- *access to illegal / inappropriate materials*
- *inappropriate on-line contact with adults / strangers*
- *potential or actual incidents of grooming*
- *in-line bullying*

Teaching and Support Staff

Staff should act as good role models in their use of digital technologies, the internet and mobile devices. In lessons where internet use is pre-planned, it is best practice that students 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. Staff are responsible for ensuring that:-

1 *They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices*
2 *They have read and understood the safeguarding portfolio of policies.*
3 *They report any suspected misuse or problem to the Headteacher / Deputy Headteacher / Senior ICT Technician or DSL for investigation / action / sanction*
4 *All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems in accordance with 'Code of Conduct' and other relevant policies*
5 *E-safety issues are embedded in all aspects of the curriculum and other activities*
6 *They monitor the appropriate use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement the school's Behaviour policy with regard to these devices*
7 *In lessons where internet use is pre-planned students / 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*
8 *Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit*
9 *It is accepted that from time to time, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Senior ICT Technicians can temporarily remove those sites from the filtered list for the period of study. Any request should have clear reasons for the need which should be explained to SLT and a log record kept of the request*

Students

- Are responsible for using the school's digital technology systems in accordance with the ICT Acceptable Use Policy issued to all students upon arrival at Aylesford School
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers
Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will help parents understand these issues through parents' evenings, newsletters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

Community Users
Community Users who access school systems / website / VLE as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

E-Safety Curriculum
Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum where relevant - and staff should reinforce e-safety messages across the curriculum where relevant. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- *A planned e-safety curriculum will be delivered as part of the ICT and Computing curriculum, the Ethics curriculum (where relevant,) and year periods (as per calendared schedule). E-Safety issues may be taught in other lessons too where relevant*
- *Key e-safety messages will be reinforced in the assemblies and other activities*
- *Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information*
- *Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet*
- *Students should be helped to understand the need for responsible use both within and outside school*

CPD – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:-

A planned programme of e-safety training will be made available to staff as a part of our CPD programme. This will be regularly updated and reinforced. It is expected that some staff may identify e-safety as a training need within the performance management process.

All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.

The DSL and Head of ICT will attend external training events (as required) and will review guidance documents released by the DfE and other relevant organisations.