GLOUCESTERSHIRE COUNTY COUNCIL

Alderman Knight School
Ashchurch Road
Tewkesbury
Gloucestershire
GL20 8JJ
Head Teacher: Clare Steel

E – Safety Policy

Date Reviewed	January 2021
Reviewed By	H Shaw
Next Review Due	January 2022
Ratified by Governors	

E-Safety Policy

January 2021

Table of Contents

Defining E-Safety 3

Scope of the E-Safety Policy 3

Teaching and Learning 4

Management of Internet Access 7

- Supervised Internet Access 7
- Information System Security 7
- Use of Email 7
- Publishing Content 7
- Filtering of Content 8
- Monitoring of Content 8
- Use of Emerging Technologies 8

Dissemination of E-Safety Information 9

- Sharing the E-Safety policy with pupils 9
- Sharing the E-Safety policy with staff 9
- In the event of pupils being unintentionally exposed to undesirable materials. 10
- In the event of pupils intentionally accessing undesirable materials. 10
- In the event of adults intentionally accessing undesirable materials. 10
- Examples of undesirable materials 10
- Training

Personnel with Direct Responsibility for the ICT Internet Facility 10

Defining E-Safety

E-safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate pupils and staff about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control and make informed decisions about their online experiences.

The school's e-safety policy will operate in conjunction with other policies including the Behaviour, Bullying and Hate, Curriculum, Acceptable Use, Safeguarding and Data Protection policies.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the schools Internet service provider, South West Grid for Learning (SWGfL)
- National Education Network standards and specifications.

Scope of the E-Safety Policy

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

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of school, but is linked to membership of the school.

The school will deal with such incidents within the parameters of this policy and the associated 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.

The Designated Safeguarding Lead and other associated staff will be trained in e-Safety issues and be aware of the potential serious child protections issues that could arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils at Alderman Knight School may be particularly vulnerable to e-safety risks due to their Special Educational Needs. These are challenging and complex issues which need to be specifically addressed through focused teaching sessions, strong pastoral support and an appropriate curriculum.

Examples of how our pupils may be more vulnerable include:

- Some pupils may make literal interpretations of content, which will affect how they respond.
- Some pupils may not understand some of the terminology
- Some pupils may have difficulties understanding relationships and social situations and therefore may be unsure who to trust.
- Some pupils may not know how to make judgements about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
- Some pupils may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.
- In addition, some pupils may not appreciate how their own online behaviour may be seen by someone else as bullying or inappropriate.

Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the National curriculum and a necessary tool for staff and pupils. It enhances and enriches the learning experience.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. They will be educated in recognising bias and possible fraudulent or fake websites. The school Internet access is designed for student use and includes filtering appropriate to the age of pupils. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Across the different Key Stages E-safety is taught through different aspects of the National Curriculum including Computing and Relationships and Sex Education and Health Education.

The aim of the Computing national curriculum ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world. Aspects of E-safety are covered in the following key stages:

KS2

- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact;

KS3

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.

KS4

- Understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns.

In addition to E-safety being an important part of the Computing National Curriculum it is also part of the new Relationships and Sex education (RSE) and Health Education curriculum which is compulsory from April 2021

By the **end of primary school**, pupils will know:

RSE

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Health Education

- That for most people, the internet is an integral part of life and has many benefits.
- To know about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices, and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Why social media, some computing games and online gaming, for example, are age restricted.
- That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

Health Education

As well as revisiting and reinforcing the objectives covered in primary, secondary pupils will:

- Know the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising information is targeted at them and how to be a discerning consumer of information online.

E-safety is also included in the PSHE and Preparation for Adulthood curriculum in post 16 and is taught as part of life-skills challenges on a Thursday and Friday.

Some examples of resources, teaching materials and topics used to deliver online safety:

Primary

- Hectors World https://www.thinkuknow.co.uk/4_7/hectorsworld
- Be Smart Online https://www.childnet.com/resources/be-smart-online
- Jessie and Friends https://www.thinkuknow.co.uk/parents/jessie-and-friends/
- BBC Bitesize https://www.bbc.co.uk/bitesize
- https://www.pshe-association.org.uk/

KS3

- Stranger Danger
- PEGI Ratings https://pegi.info/page/pegi-age-ratings
- Digital footprints and intellectual property
- STAR SEND toolkit - https://www.childnet.com/resources/star-send-toolkit/star-films
- Band Runner https://www.thinkuknow.co.uk/8_10/
- BBC Bitesize https://www.bbc.co.uk/bitesize
- https://www.pshe-association.org.uk/

KS4

- Physical and Digital Security
- Scamming
- Identity Theft
- GDPR
- Cipher
- Thinkuknow https://www.thinkuknow.co.uk/
- BBC Bitesize https://www.bbc.co.uk/bitesize
- https://www.pshe-association.org.uk/

All KS4 pupils achieve an external qualification at an appropriate level covering online safety and validated by TLM.

All pupils taught 'be SMART online' rules (Childnet https://www.childnet.com/young-people/primary/get-smart) as part of their IT and PSD lessons. Posters of the 'be SMART online' are displayed in every classroom.

Be SMART online
S afe
M eet
A ccepting
R eliable
T ell

There is a simplified version of the SMART rules for primary pupils and those with a greater learning need.

Management of Internet Access

All staff must read and agree to the 'Staff Acceptable Use Policy' before using any school ICT resources. This is required when logging onto the School network for the first time and at subsequent intervals after. The school maintains a current record of all staff and pupils who are granted access to school ICT systems. This is held by the Network Manager, Mr Jarvis.

Supervised Internet Access

- All pupils must be supervised at all times when using an Internet-enabled device
- The school may take the decision to limit access to the Internet for some pupils, where it is deemed appropriate. Examples of such circumstances are when pupils have been accessing inappropriate content, or when not following safe practices.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and is updated regularly.
- Access is only available to those with a password protected user account.

Use of Email

Users of school provisioned email will comply with the following points of policy:

- Email sent to an external organisation should be written carefully and checked before sending.
- The forwarding of chain letters or email is not permitted.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must follow the ICT Code of Conduct and Acceptable Use Policy
- Staff must follow the Acceptable Use Policy.
- When using email, staff must only use school email when contacting pupils or parents, and must not use any personal email or social media accounts.
- Some pupils in Key Stage 4 may be given a school e-mail account. They will receive training for this in ICT lessons.
- Pupils must only send e-mail when directed by a teacher as part of a planned learning activity. Any further necessary contact must be approved by both the Head Teacher and the pupils parents/carers.
- A pupil agreement is discussed and agreed before email is used.

Publishing Content

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs that include pupils will be selected carefully. Pupils' full names will not be used

on the Website or other sites, particularly in association with photographs, unless permission is given by the parent or carer.

Security

Pupils are advised never to give out personal details of any kind which may identify them or their location.

Pupils are advised on security and encouraged to set strong passwords, deny access to unknown individuals and block unwanted communications. Pupils will be educated to be responsible and to invite known friends only and deny access to others. This is delivered through our e-safety programme. The e-safety programme is comprehensive and uses guidance from the British Computer Society. This includes the benefits and risks of using the Internet, reporting of and responding to e-safety issues, protecting yourself online and the devices you use, and legal issues using and downloading from the internet.

Filtering of Content

The school will work with the Local Authority, Department for Education and the Internet Service Provider (SWGfL) to ensure filtering systems to protect pupils are reviewed and improved. This will be undertaken by the Network Manager.

- The School will block/ filter access to social networking sites and to chat rooms. This includes Facebook, Twitter, Tik Tok and Instagram.
- Pupils and parents will be made aware that the choice of social network spaces used outside school should be appropriate to the age of the student, and that many popular social networking spaces are suitable only for children over 13 years. Parents/carers should also be aware that due to our pupils needs they may be more vulnerable and it may not be appropriate for them to access such material from 13 years of age.
- Parents will be made aware that they should regularly and carefully monitor their child's access and use of social networking spaces.

If staff or pupils discover an unsuitable site, it must be reported to the Network Manager. This can then be added to the filter list.

The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Alderman Knight School cannot accept liability for the material accessed, or any consequences of Internet access.

Monitoring of Content

The school has the right to use online monitoring systems (such as E-Safe) which can monitor, manage and protect anyone using ICT at school. Such software will 'flag' inappropriate use of the school's ICT system. Examples of inappropriate use are the viewing of pornography, engaging in discriminatory behaviour or online bullying.

Use of Emerging Technologies

Emerging technologies will be examined for educational benefit by the Network Manager and the Senior Team before use in school is allowed. This will be regularly reviewed by the ICT working group.

Dissemination of E-Safety Information

Sharing the E-Safety policy with pupils

- ICT/ e-safety guidelines are posted in all rooms that contain ICT equipment.
- Pupils are informed that network and Internet use may be monitored.
- An e-safety programme is planned and delivered to all year groups with frequent reminders through various subject areas. This provision will be regularly reviewed.

Sharing the E-Safety policy with staff

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should use a school phone or computer where contact with pupils/ parents is required and not a personal device.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Sharing the E-Safety policy with parents/carers

- The School E-Safety Policy is shared on the school website and is available from the school office.
- Annual e-safety information sessions are delivered for parents and carers.
- Training is offered through the National Online Safety portal
- Parents/carers are informed of any incidents that occur in school

Training

All new staff members will receive training, as part of their induction, on e-safety and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Staff are offered an online course on internet safety throughThe National Online Safety https://nationalonlinesafety.com/training

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

E-Safety Breaches

In the event of pupils being unintentionally exposed to undesirable materials.

- The pupils should know to notify a teacher immediately; e-Safety rules are displayed in all classrooms with computer and internet access.
- The Network Manager will be notified by the teacher as soon as reasonably practicable.
- The Network Manager will contact the school's internet service provider and/or Local Authority, if appropriate, if there are concerns regarding safe use of the Internet
- Parents/carers and governors will be notified at the discretion of the Head Teacher according to the degree of seriousness of the incident. E.g. Exposure to materials that include common profanities may not be notified to parents whereas exposure to materials that included pornographic images may be.

In the event of pupils intentionally accessing undesirable materials.

All pupils will be made well aware of the seriousness of intentionally accessing undesirable materials on the internet and either viewing in school [or on mobile devices within the school grounds]. Any incident will be treated as a disciplinary matter and will be managed through the school behaviour system. The Police will be contacted in all cases where a crime has been committed or has been suspected of being committed.

In the event of adults intentionally accessing undesirable materials.

Deliberate access by any adult to unacceptable material will be treated as a disciplinary matter. Governors will be made aware immediately and the school's internet service provider and the local authority may be consulted. The Police will be contacted in all cases where a crime has been committed or has been suspected of being committed.

Examples of undesirable materials

- Pornographic images or obscene text on ICT equipment
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on websites, mobile phones or emails
- Racist, exploitive or illegal materials or messages on websites, mobile phones or emails

Personnel with Direct Responsibility for the ICT Internet Facility

E-Safety Co-ordinators: Alex Cameron

Designated Safeguarding Leads: Clare Steel, Ceri Jones and Alex Cameron

Network & ICT Manager: Mark Jarvis

Alderman Knight School aims to create and maintain a safe environment for children and to manage situations where there are child welfare concerns. The school has clearly laid down and recognised procedures for dealing with abuse or suspected abuse which is in line with recommendations made by the Gloucestershire Safeguarding Children Executive**.** Please refer to the school's Safeguarding Children/Child Protection Polic

Timetable for Review	Annually	2 Years	3 Years	4 Years
Status	Statutory	Gloucestershire CC		School
Circulation	Website	Weduc	SAM	School Office

Table of Review and Modifications

(E - Safety)

Date Reviewed	Page Number of Changes	Summary of Changes Made