Esafety and ICT Usage Policy

Last reviewed: May 2019	**Next review: May 2021**
Linked Governor: Julie Laws	**SLT Member: Rich Peters**

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Senior Leadership Team to account for its implementation. The Governing Body will be updated regularly on online safety and monitoring by the designated safeguarding lead (DSP).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (referred to as the Designated Senior Person or DSP)

Details of the school's DSP are set out in our child protection policy. The DSP takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network manager

The Network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Working with the DSP to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics 4
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09- 17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Students will be taught about online safety as part of the curriculum, including through:

- the PSHE and Computer Studies curriculum
- participation in e-safety events

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Students will be taught to:

- Use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise acceptable and unacceptable behaviour, inappropriate content, contact and conduct, and know how to report concerns
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during Parent Information Evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of Year or DSP.

6. Cyberbullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class or tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained. The DSP will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSP or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2).

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites and all activity undertaken by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them at any time on the school grounds unless the teacher grants that permission. Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2 of this document.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others.

They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any removable storage used by staff must not contain any personal information about staff or students. This information should be kept on the cloud storage provided by the school.

If staff have any concerns over the security of their device, they must seek advice from the Network manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a student/child misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use 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).

The DSP and Safeguarding Team 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 policy.

12. Monitoring arrangements

The DSP and Safeguarding Team log behaviour and safeguarding issues related to online safety.

The school make use of a variety of technologies to log and filter the following activities as part of our filtering service.

- Online Activity
- Device Activity
- Email Activity

Appendix 1: Acceptable Use Agreement: Students

[A copy of this is included within the school's Admission Documentation]

ICT, including the internet, Ashlyns' Portal, e-mail and mobile technologies, is an important part of learning at Ashlyns. We expect all students to be safe and responsible when using ICT. It is essential that students are aware of eSafety and know how to stay safe when using any type of ICT.

Students are expected to read and discuss this agreement with their parent or carer and then sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Form Tutor.

1. I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes
2. I will not download or install software on school technologies
3. I will only log on to the school network, other systems and resources with my own user name and password
4. I will follow the school's ICT security system, not reveal my passwords to anyone and change them regularly.
5. I will make sure that all ICT communications with students, teachers or others is responsible and sensible
6. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
7. I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
8. I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
9. I am aware that when I take images of students and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
10. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
11. I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
12. I will respect the privacy and ownership of others' work on-line at all times
13. I will not attempt to bypass the internet filtering system
14. I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
15. I will not sign up to online services until I am old enough to do so
16. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
17. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted

Student and Parent/Carer signature

We have discussed this document and ________________________(student's name) agrees to follow the safety rules and to support the safe and responsible use of ICT at Ashlyns.

Parent/Carer Signature:__________________________Student Signature:____________________

Appendix 2: Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Senior Finance and Operations Manager

- □ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- □ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- □ I will ensure that all electronic communications with students and staff are compatible with my professional role
- □ I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students
- □ I will only use the approved, secure email system(s) for any school business
- □ I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- □ I will not install any hardware or software without permission of the Network Manager
- □ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- □ Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- □ Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- □ I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- □ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- □ I will respect copyright and intellectual property rights
- □ I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute or offend members of the school community
- □ I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies
- □ I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, unless as agreed by a member of the Senior Leadership Team as required for the performance of my role
- □ I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …………………………………… Date ……………………

Full Name ……………………………………………………………... (printed)

Job title ……………………………………………………………………