



## ONLINE SAFETY AND ACCEPTABLE USE OF ICT

---

### Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communications help teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access.

The use of these exciting and innovative tools in school and at home has shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the risks they may face include:

- Access to illegal, harmful or inappropriate images/content
- Unauthorised access to, or loss of personal information
- The risk of being subject to grooming with people they contact on the Internet
- Sharing or distribution of personal images without consent or knowledge
- Cyber-bullying
- Access to unsuitable games
- An inability to evaluate the quality and accuracy of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading
- Excessive use which may impact on social and emotional wellbeing and development

As with all other risks, it is impossible to eliminate these completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

### Scope of this Policy

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

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents and inappropriate behaviour that takes place out of school.

### Ethos

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the 'Every Child Matters' agenda apply equally to the 'virtual' or digital world. 'The Keeping Children Safe in Education' document sets out the legal duties that must be

followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of school and its everyday practices and procedures. All staff have a responsibility to support online safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach online safety protocols.

Online safety is a partnership concern and is not limited to school premises, school equipment or the school day. The Education and Inspections Act 2006 empowers Headteachers 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 means that we will intervene in incidents that also occur outside of school if brought to our attention. Bullying, harassment or abuse or any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Anti-bullying Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

## **Roles and Responsibilities**

The Headteacher is responsible for ensuring the safety (including Online Safety) of all members of the school community.

The Computing Subject Leader (Mr R Hutton) will work with the Headteacher (Mrs T Wright) and the designated Safeguarding Leads (Mrs T Wright, Mrs J Jeffries and Mrs E Patman) to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

### The Role of Governors

- To approve and review the effectiveness of the Online Safety and Acceptable Use of ICT Policy
- The Safeguarding Governor (Miss A Cole) works with the Online Safety Lead (Headteacher) to carry out regular monitoring, including of the effectiveness of filtering and monitoring systems, and report to the Governors

### The Role of the Headteacher and Senior Management Team

- Ensure that all staff receive suitable CPD to carry out their Online Safety roles
- Create a culture where staff and learners feel able to report incidents
- Ensure that there is a progressive Online Safety curriculum in place
- Ensure that there is a system in place for monitoring Online Safety
- Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil
- Ensure that the school infrastructure/network is as safe and secure as possible
- Ensure that policies and procedures approved within this policy are implemented

### The Role of the Online Safety Lead (Mrs T Wright, Headteacher)

- Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate
- Lead the establishment and review of Online Safety procedures and documents
- Lead and monitor a progressive Online Safety curriculum for pupils
- Ensure all staff are aware of the procedures outlined in policies relating to Online Safety
- Provide and/or broker training and advice for staff
- Meet with the Senior Management Team and Safeguarding Governor to regularly discuss incidents and developments

- Coordinate work with the school's designated Safeguarding Lead including contributing to the annual Safeguarding Audit by completing the Online Safety section
- Review filtering and monitoring reports

#### The Role of Teaching Staff and Support Staff

- Participate in any training and awareness raising sessions
- Ensure all digital communications with pupils/parents/carers are on a professional level and only carried out using official school systems
- Read, understand and sign the Online Safety and Acceptable Use of ICT policy
- Act in accordance with the Online Safety and Acceptable Use of ICT policy
- Report any suspected misuse or concerns to the Online Safety Lead (Headteacher) and check this has been recorded
- Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum
- Model the safe use of technology
- Monitor ICT activity in lessons, extracurricular and extended school activities
- Demonstrate consistently high standards of personal and professional conduct especially in relation to the use of social networks, making sure that these are in line with school ethos and policies including at the time of a critical incident

#### The Role of Pupils

- Read, understand and sign the Pupil Acceptable Use of ICT Agreement
- Participate in Online Safety activities, follow the Acceptable Use of ICT Agreement and report concerns for themselves or others
- Understand that the Online Safety and Acceptable Use of ICT Policy covers actions out of school that are related to their membership of the school

#### The Role of Parents and Carers

- Endorse (by signature) the Pupil Acceptable Use of ICT Agreement
- Discuss Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet
- Access the school website in accordance with the relevant school Acceptable Use of ICT Agreement
- Keep up to date with issues through newsletters and other opportunities
- Inform the Headteacher of any Online Safety issues that relate to the school
- Maintain responsible standards when using social media to discuss school issues

#### The Role of the Technical Support Provider

- Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack
- Ensure users may only access the school network through an enforced password protection policy
- Maintain and inform the Senior Leadership Team of issues relating to filtering and monitoring
- Keep up to date with Online Safety technical information and update others as relevant
- Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Lead (Headteacher) for investigation
- Ensure monitoring systems are implemented and updated
- Ensure all security updates are applied (including anti-virus and Windows)
- Sign an extension to the Staff AUP detailing their extra responsibilities

#### The Role of Community Users

- Sign and follow the Guest/Staff Acceptable Use Policy before being provided with access to school systems

### **Effective and Efficient Deployment of ICT Resources**

ICT resources are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment.

To enable regular and whole class teaching of ICT the school has an ICT suite which all classes from Year 1 upwards use for approximately one hour per week to develop their ICT skills.

To support the cross curricular nature of ICT at least one laptop is also located in each class and linked to an interactive whiteboard.

I Pads are also located in all Infant and Junior classes and are used across the curriculum.

## **Email**

Children will:

- Have equal access to email in a safe and secure environment
- Children will be taught all the skills to use Internet and email as an ICT tool
- Children will use Internet and email to support, enhance and develop all aspects of the curriculum
- Children will develop Internet and email skills at the appropriate level regardless of race, gender, intellectual, emotional or physical difficulties

## **Guidance for All Users**

Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend ICT use, as appropriate, within the curriculum. They should model appropriate and effective use and provide guidance and instruction to pupils in the acceptable use of the Internet.

Pupils are responsible for their good behaviour on the school networks.

- While the use of information and communication technologies is a required aspect of the National Curriculum, access to the Internet is a privilege – not a right. ICT access will be given to pupils who act in a considerate and responsible manner and may be withdrawn if they fail to maintain acceptable standards of use
- Staff should ensure that pupils know and understand that, in addition to the points found under online activities which are not permitted on pages 4 and 5 of this document, no Internet user is permitted to:
  - Retrieve, send, copy or display offensive messages or pictures.
  - Use obscene or racist language.
  - Harass, insult or attack others.
  - Damage computers, computer systems or computer networks.
  - Use another user's password.
  - Trespass in another user's folders, work or files - Use the network for commercial purposes.

## **Online Safety – Education of Pupils**

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. The school has a detailed map of Online Safety education provision across all year groups.

Within this:

- Key Online Safety messages are reinforced through assemblies, Safer Internet Day, Anti-Bullying Week and throughout all lessons.
- Pupils are taught that for most people the Internet is an integral part of life and has many benefits

- Pupils are taught 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.
- Pupils are taught 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.
- Pupils are taught why social media, some computer games and online gaming for example, are age restricted
- Pupils are guided to use age-appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- In lessons where Internet use is pre-planned, younger pupils are guided to sites checked as suitable for their use. Junior pupils are given guidance to make these decisions under supervision
- The school has the highest level of firewall software inline to the broadband connection. Processes are in place for dealing with any unsuitable material that is found in internet searches, which include informing the provider in order to block content immediately
- Pupils are taught how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Pupils will sign an Acceptable Use of ICT Agreement when they join the school, which will be shared with parents and carers
- Pupils are educated to know 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. They are taught to recognise and respond appropriately to different forms of bullying, including cyber-bullying and where and how to report concerns and get support with issues online
- Pupils in years 5 and 6 visit 'Warning Zone' biannually to take part in practical workshops relating to Online Safety
- Outside agencies are employed when appropriate (for example a year 6 workshop) to give further guidance on Online Safety at age-appropriate levels

Further details on the school's response to online safety are outlined in the school's Safeguarding and Child Protection Policy as well as on the website. Here you will find links to useful websites detailing practical advice and resources as well as factsheets on Online Safety published by Lincolnshire Safeguarding Children's Board.

### **Principles for Acceptable Use of the Internet**

Use of school computers/iPads by pupils must be in support of the aims and objectives of the school's Curriculum.

Online activities which are encouraged include:

- The use of email for communication
- Use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development
- The development of pupils' competence in ICT skills and their general research skills
- Safe use of all aspects of ICT

Online activities which are not permitted include:

- Searching, viewing or retrieving materials that are not related to the aims of the curriculum
- Copying, saving or redistributing copyright-protected material, without approval
- Subscribing to any services or ordering any goods or services, unless specifically approved by the school
- Playing computer games or using other interactive 'chat' sites unless specifically approved by the school

- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages)
- Publishing, sharing or distributing any personal information about a user (such as: home address, email address, phone number, etc.), without that person's permission.
- Downloading software
- Any other activity that violates a school rule

### **Supervising and Monitoring of Internet Usage**

- Teachers should guide pupils toward appropriate materials on the Internet. This will avoid time wasting as well as going some way towards monitoring the sites accessed by pupils.
- Internet access for pupils should be available only on computers/iPads that are in highly used areas of the school such as classrooms or the ICT suite. Machines, which are connected to the Internet, should be in full view of people circulating in the area.
- Pupils should never use Internet services without close supervision.
- Pupils should always be supervised when using the Internet.
- Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored to be absolutely private. An email is as private as a postcard; it is quite likely that no one other than the sender and receiver will ever read it, but others could if they were inclined.
- Children have access to Espresso through the portal provided by school. This provides videos, English, Maths and Science activities which can be completed at home. Pupil passwords can be found in their homework diaries and the school is able to monitor use through the staff access facilities.

### **Misuse of the Internet and other ICT Resources**

Incidents of misuse of mobile phones/websites/email occurring in school should be reported immediately. Pupils should report such incidents to a member of staff, members of staff should report these to the ICT Lead/Headteacher. All such incidents will be logged in accordance with the School's Discipline Policy and Safeguarding and Child Protection procedures.

- Unfortunately, certain individuals perceive email as a way to send secret offensive messages. Anyone receiving unwanted email should report it immediately to their teacher
- The use of Facebook and other such social networking sites is forbidden in school other than in a dedicated lesson with a class teacher
- Out of school it is down to parental choice and the National legal age limit of 13. If any type of slander or malicious content does occur the school cannot be held liable
- Should there be issues arising from the misuse of the Internet at a private address (i.e., anywhere other than at AHS), but involving a pupil(s), we will endeavour to help solve the problem. We will alert parent(s) by letter, giving any details of the complaint we can, concerning date, time and location of the posting etc. We will not interview or discuss allegations with a child/children Without a parent/carer and second member of staff being present. We will not attempt to investigate the matter ourselves. If parents wish to contact their internet provider, Police, Facebook or ICT support professional they are, of course, at liberty to do so
- School cannot take responsibility for use of the Internet at home. We recommend that children at School do not have access to social networking sites and adhere to the National legal age limit of 13. However, should they do so, such activity is best supervised by a responsible adult. All staff must take great care in their online content and who is on their contacts lists
- Cameras are only to be used under supervision (refer to Anti-bullying and EYFS policies)
- Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

## Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
- Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g., telling a trusted adult, online bully box, Childline phone number 0800 1111. Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence
- All incidents of cyberbullying reported to the school will be recorded by the school. The school will follow procedures to investigate incidents or allegations of cyberbullying. The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police. Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's E-Safety ethos
- Consequences for those involved in cyberbullying will follow those for other bullying incidents and may include:
  - The bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
  - Internet access being suspended at the school for a period of time. Other consequences for pupils and staff may also be used in accordance with the schools Anti-bullying, Behaviour policy or Acceptable Use of ICT policy
  - The parent and carers of pupils being informed
  - The police being contacted if a criminal offence is suspected

## Mobile Devices

The school has a clear policy against children bringing in their own smart technology, including mobile phones, tablets and any other mobile smart device. Any child found with such a device will have the device removed from them for the day and securely stored in school. Parents will be contacted and asked to collect the device, ensuring that it does not come back into school in the future. Pupils are not permitted to wear Smart watches in school.

If there is a plausible reason why a child may need a phone in school, it is to be kept in the school office and not by the child or class teacher.

Staff must ensure that personal mobile phones are locked with a security pin code. They must be stored securely and not be accessible to pupils. All phones should be switched off or on silent during work hours and only accessed during authorised breaks. Any urgent phone calls can be made through the office. If for any reason a member of staff needs to use a mobile phone during working hours prior authorisation from the Headteacher is needed.

The school recognises online abuse may also take place outside school and that many children now have unlimited and unrestricted access to the internet via mobile phone networks, which some of them may abuse to harass, including sexually, their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content. The school has a robust programme for Online Safety in place as detailed in the Acceptable Use of ICT policy. Staff receive regular training in Online Safety and regular workshops are held for parents. The school website contains information for parents on how to protect their children online and how to educate in the safe use of online technology. The school works with the Stay Safe Partnership Team and Lincolnshire County Council to give additional online safety education to the children.

The Staff Code of Conduct provided further advice and guidance regarding the use of social networking and electronic communication with young people in our care.

## **Chatrooms**

Pupils will not be allowed access to public or unregulated chat rooms. Children should use only regulated educational chat environments where an educational benefit has been established. If used this will always be supervised and the importance of chatroom safety emphasized.

## **Filtering and Monitoring External Websites**

It is a requirement that access to the Internet provided to staff and pupils in any school or educational institution through any Internet Service Provider (ISP) is a blocked or filtered service. The following filters are in place:

- All school devices connected to the Internet are protected by the Securly filtering system (provided by Ark). Securly issues weekly reports to the Headteacher detailing all blocked activity on the school system. This is checked weekly by the Headteacher and ICT Lead to establish whether any pupil has made deliberate attempts to access inappropriate materials.
- All school devices connected to the Internet are monitored by the Senso monitoring system (provided by Ark). Senso provides weekly reports to the Headteacher detailing any attempts to access inappropriate materials. Should someone attempt to access materials considered dangerous, the Headteacher is notified immediately by email and will take appropriate action.
- Email Spam and malicious content is done by the built in Microsoft Office 365 Tenant, this is always in an update cycle
- MFA is switched on for access to Office 365 email for all adults
- All devices with Windows have Avast Antivirus to protect against malware/viruses. This is also regularly updated with daily definitions updates

The effectiveness of the school filtering and monitoring procedures is regularly reviewed by the ICT Lead and Headteacher.

We advise parents that we provide filtered and monitored access to the Internet for pupils. However, they should also be aware that with these emerging and constantly changing technologies there is no absolute guarantee that a pupil cannot access materials that would be considered unsuitable. The chance of just coming across such materials is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. If you are unfortunate enough to come across any offensive web pages, whilst using school equipment, you are to make a note of the address and report it to the Headteacher immediately. The ICT staff will then take the appropriate action to block the site.

## **School Website**

- There is a person within school who has been designated as website/virtual learning environment editor. Any materials to be put on the website / Virtual Learning Environment should be passed to them first. This person is Mrs Wade
- If any outside agent is helping the school to develop their website, then the designated person must maintain a strong dialogue with them and ensure that they see the final product before it goes live
- The Headteacher and Governors will make decisions about what they consider to be suitable and appropriate on the school website / Virtual Learning Environment
- Only images of pupils in suitable dress will be used in order to reduce the risk of inappropriate use

## **Appropriate Legislation, Including Copyright and Data Protection**

All software loaded on school computer systems must have been agreed with the designated person in the school. All our software is used in strict accordance with the licence agreement.



We do not allow personal software to be loaded onto school computers. Please refer to the school's Data Protection Policy.

### Health & Safety

At AHS all ICT equipment is used in compliance with Health & Safety requirements. All electrical equipment is checked, any concerns are passed onto the Headteacher. We will operate all ICT equipment in compliance with Health & Safety requirements. Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers.


Staff must not make inappropriate contact with pupils by electronic methods (see Staff Internet Guidance in Code of Conduct), nor must they take and store any electronic images of children on any personal device. Images taken for School purposes, e.g. For EYFS records, School prospectus, newsletter, website and the AHS Facebook page must be taken with the school's own cameras only. Images are stored only on school computers and must not be taken off premises by staff in electronic form and only with permission in paper form.

Parents sign to give permission for video and images to be used while a child is at school and for their use in the school newsletter, website, press articles, AHS Facebook page and any other social media platforms.

**This policy was approved by the Governing Body on**

Signed:  \_\_\_\_\_ Chair of Governors Date: 23.01.2024

Signed:  \_\_\_\_\_ Safeguarding Governor Date: 23.01.2024

Signed:  \_\_\_\_\_ Headteacher Date: 23.01.2024

**This policy must be read in conjunction with other related School policies:**

- **Safeguarding and Child Protection Policy**
- **Data Protection Policy**
- **Anti-bullying Policy**
- **Behaviour Policy**
- **Staff Code of Conduct**
- **Staff social media Policy**
- **Parent social media Policy**

***Any reference to the word 'School' implicitly includes all ICTs associated clubs/activities including Kids Club. This policy also applies to EYFS***

PREPARED BY	AUTHORISED BY	LAST REVIEWED	REVIEW DATE	NO. OF PAGES
Ralph Hutton	Theresa Wright	Spring 2024	Spring 2025	9

## Appendix 1

### AYSCOUGHFEE HALL SCHOOL

#### Responsible Internet Use

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any website unless my teacher has already approved that site.
- I will only sign in using my own username.
- I will not look at or delete other people's files.
- I will not bring CD-ROMs, data sticks, personal iPads, or Laptops into school. (Work completed at home can be sent in via email to [work@ahs.me.uk](mailto:work@ahs.me.uk). All work should be marked for the attention of your class teacher).
- I will only e-mail people I know, or those my teacher has approved.
- Any messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, nor will I arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I know that the school may check my computer files and may monitor the Internet sites that I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

# AYSCOUGHTEE HALL SCHOOL



## General Data Protection Regulation – Parental Consent Form

Name of Child:.....Class .....

Occasionally, we may take photographs of the children at our school. We may use these images in our School's prospectus or in other printed publications that we produce, as well as on our website. We may also make video recordings for school performances.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other interesting event. Pupils will often appear in these images, which may appear in local newspapers, or on televised news programmes.

To comply with the General Data Protection Regulation 2018, we need your permission before we can photograph or make any recordings of your child. Please answer the questions below then sign and date the form where shown. If there are any queries, please do not hesitate to contact the school.

Please circle your answer

The Infant and Junior productions are held at the end of the Summer and Autumn terms respectively. We seek your permission for your child to be filmed on video/photographed during the production and at other times throughout their school career at Ayscoughfee.	Yes / No
Your child may also be photographed at other times including at sporting events, on outings and sometimes whilst doing special activities in the classroom. They may feature in Press Publications and on our School Website for which your permission is also sought.	Yes / No
May we use your child's image to post on our official Facebook page 'Ayscoughfee Hall School Life'?	Yes / No

Conditions for use of these videos/photographs are on the back of this form. I have read and understood the conditions of use on the back of this form.

Signature: \_\_\_\_\_ (Parent/Carer)

Print name: \_\_\_\_\_

Date: \_\_\_\_\_

## Conditions of School Use

- This form is valid for the period of time your child attends this school. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your agreement at any time which you have every right to do.
- We, the school, will not use the personal details or full names (which means first name and surname) of any child in a photographic image or video, on our website, in our school prospectus or in any of our other printed publications used outside of the school.
- We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, Facebook page in our school prospectus or in other printed publications.
- If we wish to identify an individual child in a caption in any printed material used outside of the school, or on our website, we will seek your permission first.
- We may include pictures of pupils and teachers that have been drawn by the pupils.
- We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”.
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- As the child’s parents/guardian, we agree that if we take photographs or video recordings of our child/ren which includes other pupils, we will use these for personal and family use only. I/we will not post any photographs or video recordings of our child/ren which include other pupils on any form of social media (for example Facebook, Instagram, Snapchat).

# *AYSCOUGHTEE HALL SCHOOL*



Dear Parents,

## **Year 1 and 2 - Acceptable Use Agreement**

The School has access to the Internet and ICT is used from Year 1 upwards. For our own protection and that of the children in our care, it has been necessary to draw up an official Acceptable Use Agreement and Parent's Statement relating to the Internet. Would you please read the attached Agreement carefully and sign the relevant part of the Parent's document.

Signed statements should be returned to the main school office. Failure to do so will automatically disqualify your child(ren) from using this facility until they are returned. Access to the Internet for assessment is unaffected.

Yours sincerely

Mrs T L Wright  
Headteacher

## AYSCOUGHFEE HALL SCHOOL

### PUPILS' ACCEPTABLE USE AGREEMENT

Children in the Infants will be accompanied when using the computers, they may do individual research using the internet in Year 2.

When using the computers, all children are required to:

- Only go on to the computer by logging on as themselves.
- Not go on to other people's files.
- Only use the computers for schoolwork and homework.
- Ask permission from a member of staff before using the Internet for topic work.

If any of these rules are broken the children must report to their teacher as soon as possible and realise that they may be disciplined, but that their honesty will be recognised.

### PARENTS' STATEMENT

As the parent/guardian of ..... I acknowledge that I have read the Acceptable Use Agreement about student use of the Internet and have discussed it with my child. I understand that this access is designed for educational purposes. I understand that Ayscoughfee Hall School takes every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and systems. I further understand that my child has, and will continue to receive, online safety education to help them understand the importance of safe use of technology and the Internet – both in and out of school. I acknowledge that, from time-to-time, unsuitable materials can penetrate even the highest levels of filtering, and should this happen, the school will take immediate action to block such materials and ensure that I am informed if my child is directly affected. In such cases where individuals **purposefully** search out inappropriate materials online the school cannot be held responsible for the nature and content of this, however, immediate action will be taken to prevent this content from being revisited.

My child may use the Internet as part of their school studies.

Signed ..... Date .....

Parents/guardian of ..... Class Teacher .....

Please return to the main school office as soon as possible.

# *AYSCOUGHTEE HALL SCHOOL*



Dear Parents,

## **Year 3 - Acceptable Use Agreement**

The School has access to the Internet and it is used from Year 1 upwards. As you are aware, for our own protection and that of the children in our care, the School has drawn up an official Acceptable Use Agreement and Parent's Statement relating to the Internet, which you will have signed in the past. From Year 3 upwards all children are requested to read carefully and then sign for themselves the attached Agreement before returning it to their teacher.

We would ask if the attached could be completed and returned to the School office as soon as possible. Failure to do so will automatically disqualify your child(ren) from using this facility until they are returned. Access to the Internet for assessment is unaffected.

Yours sincerely

Mrs T L Wright  
Headteacher

## AYSCOUGHFEE HALL SCHOOL

### PUPILS' ACCEPTABLE USE AGREEMENT

When using the computers, I .....(enter name) will:

- Only access the system by logging on as myself.
- Not access other people's files.
- Only use the computers for schoolwork and homework.
- Not bring in CD ROMs, data sticks, personal iPads or Laptops in from home (work completed at home can be sent in via email to [work@ahs.me.uk](mailto:work@ahs.me.uk). All work should be marked for the attention of your class teacher).
- Ask permission from a member of staff before using the Internet.
- Only E-mail people I know or whom my teacher has approved.
- Only open E-mails from people that I know.
- Ask an adult to deal appropriately with E-mails from unknown addresses.
- I will not use internet chat.
- Not give my home address, or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- Report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
- The messages I send will be polite and responsible.
- I understand that the school can check my computer files and may monitor the Internet sites that I have visited.

If I break any of these rules, I will report it to my teacher as soon as possible and realise that I could be stopped from using the internet or computer, but that my honesty will be recognised.

Pupils signature ..... Date .....

Parents signature ..... Date .....