# AYSCOUGHFEE HALL SCHOOL

## ACCEPTABLE USE OF ICT

### Scope of this Policy

This policy applies to all members of the school community (staff or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

### Online behaviour

As a member of the school community, you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend or misinform other members of the school community (for example, content that is obscene, or promotes violence, discrimination, conspiracy theories or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

### Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt by any means (including by the use of a Virtual Private Network (VPN)) to circumvent the content filters or other security measures installed on the school's IT

systems, and do not attempt to access parts of the system that you do not have permission to access.

- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- Guests/visitors to the school must access the system via the guest Wi-Fi only. Please see below for joining details.

**Passwords**

Passwords protect the school's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

**Use of Property**

Any property belonging to the school should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the Headteacher or Bursar.

**Use of school systems**

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

**Use of personal devices or accounts and working remotely**

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Headteacher.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies, including the use of two-factor authentication.

**Monitoring and access**

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where

necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Pupils are not permitted to use personal devices in school at any time. Any personal devices brought into school by pupils in contradiction to this will be confiscated and may be examined if there is a significant concern relating to the content.

**Tracking Devices and Technology**

While the school is not responsible for individual settings on personal devices, [consistent with our policy on mobile device usage during school hours] our general position is that tracking technology that relies on location data sourced from third party devices should not be used on school premises or on school trips – given the potential privacy concerns for third parties.

That said, the school is aware that there may be instances where such technology – whether, for example, for security of belongings or for parents' peace of mind as to children's whereabouts – can be used appropriately and proportionately. We would encourage parents / pupils to raise any such requests with us, for example in advance of a trip, so that we can discuss appropriate usage.]

**Compliance with related school policies**

To the extent they are applicable to you, you will ensure that you comply with the school's Online Safety Policy, Safeguarding and Child Protection Policy, Behaviour Policy, Anti-bullying Policy, Mobile Phone Policy, Staff Code of Conduct and Staff Social Media Policy, Retention of Records Policy and Data Protection Policy.

**Retention of digital data**

Staff and pupils must be aware that all emails sent or received on school systems should be deleted after 3 years and email accounts will generally be closed and the contents deleted within 1 year of that person leaving the school.

Any information from email folders that is necessary for the school to keep for longer, including personal information (e.g. for a reason set out in the school privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact T Wright (Headteacher) or E Gibson (Bursar).

**Breach reporting**

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, they must notify Mrs E Gibson (Bursar) as soon as possible and certainly within 48 hours. For full details please see the school Data Protection Policy.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

**Use of Artificial Intelligence**

Ayscoughfee Hall School does not permit the use of generative AI tools such as ChatGPT on school devices/systems by pupils. The use of generative AI tools by staff is covered in the school AI Policy. In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

Ayscoughfee Hall School will evaluate the benefits and risks of any proposed use of generative AI by staff or pupils, with particular regard to risk associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the school will remain alert to the possibility of unauthorised use.

**Breaches of this policy**

A deliberate breach of this policy by staff or pupils will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person’s access to school IT systems.

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you

should report it to Mrs T Wright – Headteacher and DSL. Reports will be treated in confidence wherever possible.

**Acceptance of this policy**

**Staff, Volunteers and Visitors**

All staff and volunteers must read and sign this policy to confirm their acceptance of the terms set out within. (Appendix A)

Visitors to the school must sign into the guest Wi-Fi only:

**AyscoughfeeGuest**

**Password: Gu35tW1f1**

The guest Wi-Fi gives the same filtering and monitoring protections as children's accounts.

**Pupils**

Children may begin accessing the Internet as part of their computing lessons from Year 1. Parents of Year 1 and Year 2 children are required to discuss with and sign on behalf of the agreement shown in Appendix B before access to the Internet is permitted.

Children in years 3-6 are expected to read and sign (in conjunction with their parents) the acceptable use agreement shown in Appendix C.

**This policy was approved by the Governing Body on 30th June 2026**

***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 |
|---|---|---|---|---|
| SMT | Theresa Wright | Summer 2026 | Summer 2027 | 5 |

**Appendix A**

## Acceptance of Ayscoughfee Hall School Acceptable Use of IT Policy (Staff and Volunteers)

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Mrs T Wright (Headteacher)

I understand and accept this acceptable use policy:

Name: ……

Signature: ……

Date: ……..

**Appendix B**

## 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**

**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. 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.

Pupil's signature …… Date …….

Parent's signature …… Date …….

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