Ashton House School

Online Safety and

ICT Acceptable Use Policy

1.8

Policy Title:	**Online Safety and ICT Acceptable Use Policy**
Version:	1.8
Policy Summary:	**This Policy applies to the use of all devices and online materials in use at Ashton House School and its EYFS setting.** The term e-safety is used throughout this policy to mean use of ICT resources (computers, printers, software applications) access to and use of online materials and resources and use of mobile technology (mobile phones and tablets).
Policy Owner:	Headteacher
Relevant to:	All staff, volunteers, contractors and service providers, parents and guardians, pupils e – safety manager and co-ordinator
Date introduced:	November 2016
Next review date:	January 2024
Related School Documents:	• Acceptable Use Agreements (KS1, KS2, Staff and Parents) • Policy for Use of Social Media • Policy for Use of Mobile Phones, Cameras and Tablets • Anti – bullying Policy
Date(s) modified/reviewed:	25/1/17 modified – use of closed twitter account, visitor access to public wi fi November 2017 – reviewed – Policy Summary extended 12/07/18 modified – insertion of the term GDPR legislation Replacement of Annex D 'E Safety Form' with January 2017 version (AS) 6/2/19 – Reviewed and formatting changes (font/page numbers) 13/3/19 – modified to include the sentence – Parents are not permitted to use mobile phones or other mobile technology in the EYFS setting. 24/7/2020 – Reviewed and modified to include the sentence – Staff may use their own device e.g. laptop, chromebook or tablet in school to access the school server or teaching resources. March 2021 – Inclusion of refreshed AUP Agreement Forms for Parents, Pupils and Staff. December 2021 – amendment to wording to allow staff to use personal equipment e.g. mobile phone to take pictures when no other equipment is available and only after asking permission from a member of SLT to do so.

	October 2022 – statement added regarding the introduction of a school mobile phone to be taken on school trips January 2023 – additional statement added regarding the prohibition of internet connected watches worn by pupils in school.

ONLINE SAFETY AND ICT ACCEPTABLE USE POLICY

Introduction

This policy has been developed with particular reference to guidance and policy templates produced by The South West Grid for Learning Trust (SWGFL). The template for the policy is also recommended for use in schools by the UK Safer Internet Centre.

The term e-safety is used throughout this policy to mean use of ICT resources (computers, printers, software applications) access to and use of online materials and resources and use of mobile technology (mobile phones and tablets).

Policy Scope

The term e-safety is used throughout this policy to mean use of ICT resources (computers, printers, software applications) access to and use of online materials and resources and use of mobile technology (mobile phones and tablets).

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 is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school but is linked to enrolment of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Student Care Process.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or guardians of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Proprietor

The Proprietor is responsible for the approval of this policy and for reviewing the effectiveness of the policy. This will be carried out by the Proprietor by receiving and scrutinizing regular information about e-safety incidents and monitoring reports.
The Proprietor's role will include:

- Regular meetings with the individual designated as the E-Safety Coordinator.
- Regular monitoring of e-safety incident logs.
- Regular monitoring of filtering mechanisms that the school deploys.

Headteacher and Senior Management Team

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the individual designated as the E-Safety Coordinator.
The Headteacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff in accordance with the relevant policy.

The Headteacher and Senior Management Team are responsible for ensuring that the individual designated as the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train all other staff, volunteers, contractors and service providers.

The Headteacher and Senior Management Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Management Team will receive and scrutinize regular monitoring reports from the individual designated as the E-Safety Coordinator.

E-Safety Coordinator

The individual designated as the E-Safety Coordinator is expected to lead on e-safety issues across the whole school and EYFS setting. In particular the role requires that the following responsibilities are effectively fulfilled.

- Day to day responsibility for e-safety issues and leading in establishing and reviewing the school e-safety policies, procedures and records.
- Ensuring that all staff, volunteers, contractors and service providers are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff, volunteers, contractors and service providers.
- Liaise with the Local Authority and other relevant external agencies.
- Liaise with technical support.

- Receive reports of e-safety incidents and create and maintain a log of incidents to inform future e-safety
- Policy developments.
- Meet regularly with Proprietor, Headteacher and senior school staff to discuss current issues, review incident logs and filtering/change control logs.

The E- Safety Co-ordinator will work with Technical Support to ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any other relevant body E-Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation/action/sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- The sharing of personal data.
- Access to illegal/inappropriate materials, including extremist materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Teachers, Support Staff, Volunteers, Contractors and Service Providers

Teaching, support staff, volunteers, contractors and service providers are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation/action/sanction.
- All digital communications with pupils/parents/guardians should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the e-safety and acceptable use agreements.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where Internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Parents and Guardians

Parents and guardians play a crucial role in ensuring that their children understand the need to use the
internet/mobile devices in an appropriate way. The school will take every opportunity to help parents and guardians understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local e-safety campaigns/literature.
Parents and guardians will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events (parents are asked to sign a parental consent form)
- Access to sections of the school website/VLE and any on-line student records.
- Their children's personal devices in the school (where this is allowed).

- Parents are not permitted to use mobile phones or other mobile technology in the EYFS setting.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying, sexting, etc.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their enrolment in the school.

Policy Statements

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways.

- A planned e-safety curriculum will be provided as part of PHSE and will be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff members, volunteers, contractors and service providers will act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents and Guardians

Many parents and guardians have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their child's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and guardians through:

- Curriculum activities
- Letters, newsletters and web site
- Parents evenings/sessions
- High profile events and campaigns e.g. Safer Internet Day.
- Reference to relevant web sites and publications e.g. www.swgfl.org.uk www.saferinternet.org.uk www.childnet.com/parents-and-carers

Proprietor, Staff, Volunteers, Contractors and Service Providers

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

- The E– Safety Coordinator will receive e-safety training as part of their role, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements. The E-Safety Co-ordinator will train staff members in E– Safety.
- The school will ensure that contractors and service providers are provided with adequate e-safety training and understand the school e-safety policy and Acceptable Use Agreements.
- A planned programme of formal e-safety training will be made available to staff members and if appropriate, volunteers, contractors and service providers. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff members, volunteers, contractors and service providers at least once every two years.
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This policy and its updates will be presented to and discussed by staff in staff meetings or INSET days at least annually.
- The E-Safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as required or on request.

Technical Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical Systems.
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the school's systems, without prior written agreement.
- Users may use the following types of removable media for the purposes detailed.
    - CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
    - USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user with the permission of the Proprietor. The use of applications on this type of media is strictly prohibited.

Bring Your Own Device (BYOD)

Pupils may bring a mobile phone to school if walking home independently or similar circumstance. The phone is taken to the school office before the child goes to the classroom where it stays and it is collected at the end of the day when the pupils leaves.

Staff may use their own device e.g. laptop, chromebook or tablet in school to access the school server or teaching resources.

Pupils may use their own device e.g. Kindle or other type of e reader on the following conditions:

- The device has been approved by the class teacher or E- Safety Co-ordinator
- The device is used under the supervision of a staff member
- If the device is able to connect to the internet using a sim card or other means this feature must be disabled whilst under the school's supervision

Pupils in Years 5 & 6 may wear watches, however, any watch that has the same functionality as a mobile phone or PC, is not permitted on the school site.
Analogue and non internet connected digital watches are acceptable in school.

Visitors may use their own device e.g. tablet or laptop on the following conditions:

- No access is given to the school network
- Visitors are allowed access to the school's public wi fi network subject to all school safeguarding protocols
- Digital and Video images must not be taken unless authorized to do so

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and guardians and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate pupils about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff will inform and educate pupils about the risks associated with the taking, us, sharing, publication and distribution of images. In particular, that they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents and guardians are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents or guardians comment on any activities involving other pupils in the digital/video images.

Staff and volunteers can take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment when and where available.
A school mobile phone is available to be taken off site for Sports and Trips.
The personal equipment of staff should not be used for such purposes without the express permission of a member of the SLT and should be deleted from the personal device as soon as possible and in the presence of another staff member.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the school website, in a class email or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

Written permission from parents or guardians will be obtained before photographs of pupils are published on the school website.

Digital images of a pupil's work will only be published with the permission of the pupil and parents or guardians.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR legislation and the Data Protection Act 1998.

Staff must ensure that they.

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice.

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

- Users must immediately report, to the Headteacher – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents and guardians (email, chat, VLE etc.) must be professional in tone and content.
- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Staff personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information.

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, parents or guardians or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- The school's use of social media for professional purposes will be checked regularly.
- The use of the closed 'Twitter' account used for school journeys or similar will follow these guidelines.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the school network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the Online Safety and ICT Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the school as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the school's VLE from home, the same Acceptable Use Agreement will apply.

The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the school network, the internet or VLE in an abusive or illegal manner, a report must be made to the Headteacher immediately and then a decision will be made as to whether the allegation needs to be handled via the school staff disciplinary procedure or the Safeguarding Policy.

Appropriate and Inappropriate Use by Children or Young People

Acceptable Use Agreements detail how children and young people are expected to use the school network, the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The school will encourage parents and guardians to support the agreement with their child. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school setting that the agreement are accepted by the child with the support of the parent or guardian. This is also intended to provide support and information to parents and guardians when children may be using the Internet beyond school.

Further to this, it is hoped that parents and guardians will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents or guardians feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free. File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school.

In the Event of Inappropriate Use

Should a child be found to misuse the network or online facilities whilst at school, the following consequences will occur.

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a communication sent home to parents or guardians explaining the reason for suspending the child use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the school network or internet for a period of time.
- A communication may be sent to parents or guardians outlining the breach in Safeguarding Policy where a child is deemed to have misused technology against another child or adult.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

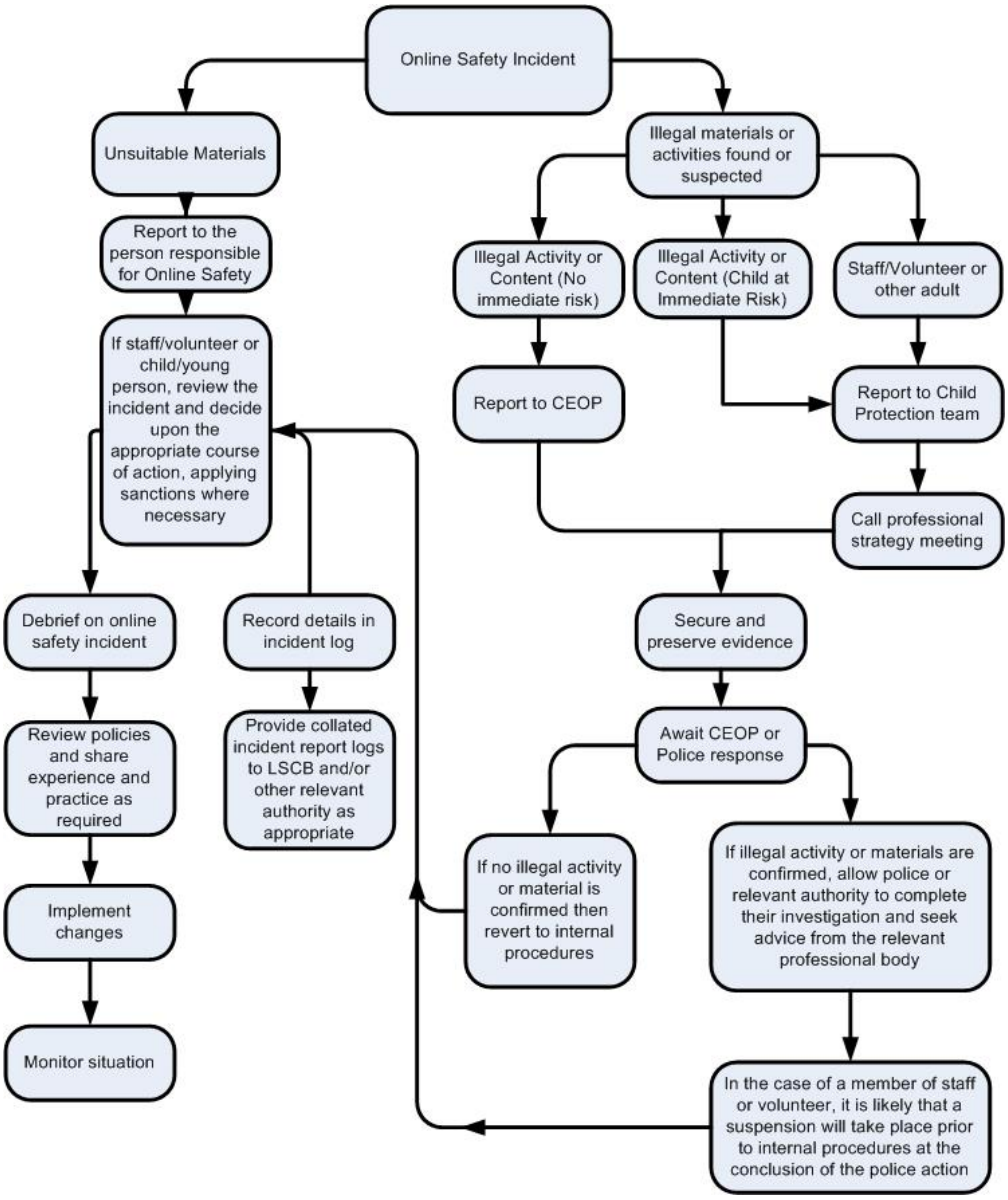
The issue of a child deliberately misusing the school network or online technologies will be addressed via the Student Care Policy or Safeguarding Policy. Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Responding to Incidents of Misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “In the Event of Inappropriate Use” above). See below flow.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart below for responding to online safety incidents and report immediately to the police.



Source: South West Grid For Learning, E-Safety E-Safety Policy Template (2016)

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed.

- Have more than one senior member of staff/volunteer involved in this process. This is
- vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young
- people and if necessary can be taken off site by the police should the need arise. Use
- the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to
- conduct the procedure, but also that the sites and content visited are closely monitored
- and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the
- content causing concern. It may also be necessary to record and store screenshots of
- the content on the machine being used for investigation. These may be printed, signed
- and retained (except in the case of images of child sexual abuse – see below).

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following.

- Internal response or discipline procedures.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be halted immediately and referred to the Police without delay. Other instances to report to the Police would include.

  - Incidents of 'grooming' behaviour.
  - The sending of obscene materials to a child.
  - Adult material which potentially breaches the Obscene Publications Act.
  - Criminally racist material.
  - Other criminal conduct, activity or materials.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment without the express permission of a member of the SLT and should be deleted from the personal equipment as soon as possible in the presence of another staff member.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- ***We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.***

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libelous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

The following Annexes are included as part of the Policy

ANNEX A: Acceptable Use Policy for PARENTS
Parent Declaration Form

ANNEX B: Acceptable Use Policy for LOWER SCHOOL PUPILS

ANNEX C: Acceptable Use Policy for UPPER SCHOOL PUPILS

ANNEX D: Acceptable Use Policy Staff Declaration Form

ANNEX E: E-Safety Incident Form (The White Form)

Ashton House School

Acceptable Use Policy (AUP) for PARENTS

What is an AUP?

We ask all children and adults involved in the life of Ashton House School to sign an Acceptable Use Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
Your child will sign a child-appropriate AUP.

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.
School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.
We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Where can I find out more?

You can read Ashton House's full Online Safety Policy on the school website ashtonhouse.com for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). The policies cover such topics as:

- Roles and responsibilities of members of the school community
- Education and curriculum
- Handling online-safety concerns and incidents
- Actions where there are concerns about a child
    - Sexting
    - Bullying
    - Sexual violence and harassment
    - Misuse of school technology (devices, systems, networks or platforms)

    - Social media incidents
- Data protection and data security
- Appropriate filtering and monitoring
- Electronic communications
- Email
- School website
- Cloud platforms
- Digital images and video
- Social media
- Device usage

If you have any questions about this AUP or our approach to online safety, please speak to a member of staff.

What am I agreeing to?

1. I understand that Ashton House School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, proprietors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video

of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant enrolment form.

7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety (NB: the recent LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety, but only half talk about it with them more than once a year). Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
9. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
10. I can find out more about online safety at Ashton House School by reading the full Online Safety Policy on the school website and can talk to my child's class teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

Ashton House School

Acceptable Use Policy (AUP) PARENT DECLARATION

Please detach this page and return to the school office.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

Ashton House School

Acceptable Use Policy (AUP) for LOWER SCHOOL PUPILS

My name is _____

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **KNOW** people online aren't always who they say	
5. I don't keep **SECRETS** just because someone asks me to	
6. I don't change **CLOTHES** in front of a camera	
7. I am **RESPONSIBLE** so never share private information	
8. I am **KIND** and polite to everyone	
9. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
10. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	

My trusted adults are:

_____ at school

_____ at home

Ashton House School

Acceptable Use Policy (AUP) for UPPER SCHOOL PUPILS

My name is _____

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use apps, sites and games if a trusted adult says I can.
2. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people; I get creative to learn and make things!
3. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
5. ***I am careful what I click on*** – I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.
8. ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
9. ***I know new friends aren't always who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are. If I want to meet them, I will ask a trusted adult, and never go alone or without telling an adult.
10. ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.

11. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
12. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
13. ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
14. ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
15. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
17. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
18. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
19. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement.
If I have any questions, I will speak to a trusted adult.

At school that includes: _____

Outside school, my trusted adults are: _____

Signed: _____ **Date: _____**

Ashton House School

Acceptable Use Policy (AUP) STAFF AGREEMENT FORM

(One copy for school and one for staff member)

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, personal devices, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Proprietor.
- I will safeguard my password(s).
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
  (This is currently: Microsoft Outlook and Google Mail)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Proprietor, Simon Turner.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission. Any images taken on a personal device will be deleted as soon as possible, this deletion will be witnessed by a fellow staff member.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named child protection officer (DSL)/ relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use school systems in accordance with any school policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a Designated Safeguarding Lead/ Deputy at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I agree to abide by all the points contained within the school's **Online Safety and ICT Acceptable Use Policy.**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

Signature: …… Date: ……

Full Name: …… (printed)

Job Title: ……

Head Teacher's Signature

Signature: …… Date: ……

Please return this document to the school office to be retained.

Ashton House School

E SAFETY INCIDENT FORM

'The White Form'

Pupil Name	Date of Birth	Year Group
Name and position of person completing form (please print)		
Date of incident / concern:		
Incident / concern details		
Where did the incident occur? (circle)	In school / Outside school	
Who was involved in the incident? (circle)	child / staff member / other (please specify)	
Type of incident: (tick)	○ bullying or harassment (cyber bullying) ○ hacking or virus propagation ○ terrorist material child abuse ○ images on-line gambling ○ illegal hard core pornographic material	○ deliberately bypassing security or access ○ racist, sexist, homophobic ○ religious hate material ○ drug/bomb making material ○ soft core pornographic material ○ other (please specify)
Description of incident*		

Continued on next page

<table>
<tr><td>Nature of incident
(tick)</td><td>Deliberate access
Did the incident involve material being?
○ Created
○ Viewed
○ Printed
○ Shown to others
○ Transmitted to others
○ Distributed
Could the incident be considered as;
○ Harassment
○ Grooming
○ Cyber bullying
○ breach of AUP</td><td>Accidental access
Did the incident involve material being?
○ Created
○ Viewed
○ Printed
○ Shown to others
○ Transmitted to others
○ Distributed</td></tr>
<tr><td>Action taken
(tick)</td><td colspan="2">○ Incident reported to head teacher/senior manager
○ Advice sought from HSCP
○ Referral made to HSCP
○ Incident reported to police
○ Incident reported to social networking site
○ Child’s parents informed
○ Disciplinary action to be taken
○ Child/young person debriefed
○ E-safety policy to be reviewed/amended
Other:</td></tr>
<tr><td colspan="3">Outcome of incident/investigation*</td></tr>
<tr><td colspan="2">Signature</td><td>Date form completed</td></tr>
</table>

*Continue on a separate sheet if necessary

Form reviewed January 2023