Ashdown
Primary School

Online Safety Policy & Acceptable Use Guidelines

Review Date: January 2026

Next review date: Spring 2027

Vision

Empower everyone to discover their potential, develop the skills to thrive with confidence and compassion, and make a positive difference in the world.

At the heart of our vision are our three key drivers:

People, Planet and Potential

People: we put **people** first. Kindness, inclusion, respect and support are the golden threads that run through our school day. Our school community is ambitious yet supportive; a place where everyone is valued and belongs.

Planet: We care deeply about our **planet** and our responsibility to protect it. We learn together how to make choices that are sustainable, kind, and thoughtful—helping children become global citizens who care about the world around them.

Potential: We believe every child and adult in our school community has **unique potential,** and it's our job to nurture it—whether that's academic, creative, social or emotional. We are an ambitious, supportive community where success is celebrated in all its forms.

Ethos Statement

We value everyone, nurture their strengths and enable them to flourish.

Values

Caring, Curious and Confident

Equal Opportunities

At Ashdown Primary School we believe that all children, regardless of first language, disability, race, gender, cultural or socio-economic background, should receive equal access to the full school curriculum.

Disability Statement

Ashdown Primary School is proud to be an inclusive school. We are able to offer access to the full curriculum for children who have a physical disability.

We have easy access into the main part of the building and have disabled toilet facilities within the school.

As with any additional needs the schools work closely with parents and appropriate outside agencies

Introduction
The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Ashdown Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Ashdown Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to responsible use of digital media for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- social media
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming)
- sexting (sending and receiving of personally intimate images)
- The 'prevent duty' in the Counter-Terrorism and Security Act 2015.

Commerce

- online gambling
- inappropriate advertising
- phishing
- financial scams.

Scope
This policy and guidance applies to all members of Ashdown Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy IT systems, both in and out of Ashdown Primary School. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the Ashdown Primary School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy and guidance, which may take place outside of the school, but is linked to membership 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

Role	Key Responsibilities
Exec Headteacher / Head of school	• To take overall responsibility for online safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)
Online safety Leader / Designated Child Protection Lead	The Online Safety Leader is a safeguarding officer (DSO) who oversees online safety at Ashdown Primary School. • takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community including regular activities in collaboration with the school's pupil digital leaders. • ensures that online safety education is embedded across the curriculum • liaises with school IT technical staff • ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident • ensures that an online safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ➢ sharing of personal data ➢ access to illegal / inappropriate materials ➢ inappropriate on-line contact with adults / strangers ➢ potential or actual incidents of grooming ➢ cyber-bullying and use of social media
Governors /safeguarding governor	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of safeguarding governor will include responsibility for Online Safety. • To support the school in encouraging parents and the wider community to become engaged in online safety activities.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the PSHE curriculum • To liaise with the Digital Leader regularly
PSHE Curriculum	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the Digital Leader regularly

Role	Key Responsibilities
Leader	
Schools ICT services provided by East Sussex County Council	• To report any online safety related issues that arises, to the Headteacher. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date. • To ensure the security of the school IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis. • To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the network remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures encrypted in a suitable location. • To ensure that all data held on pupils on the school office machines have appropriate access controls in place • To communicate regularly with SLT and the nominated safeguarding governor to discuss current issues, review incident logs and filtering / change control logs • Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements; • Know that spam, phishing and virus attachments can make e mail dangerous. We expect our SLA to ensure email communication is safe and secure, but we understand it should not be used for transferring pupil level, or sensitive information.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in all learning activities involving online technology.
All staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to this policy (Code of Conduct for IT and Computing.) and the staff code of conduct. • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the Headteacher • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems.
Pupils	• To read, understand and adhere to the Pupil Acceptable Use Guidelines (to be taught in lessons) • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Role	Key Responsibilities
	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of online safety procedures.
Parent Carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Guidelines, which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Guidelines with their children • To consult with the school if they have any concerns about their children's use of technology • Follow acceptable use procedures at school events • Follow acceptable use procedures for video calls (Zoom, Microsoft Teams etc) • Abide by the home school charter. • Role model safe and appropriate use of technology and social media. • Identify changes in behaviour that could indicate that their child is at risk of harm online.
External groups	• Any external individual / organisation will read, understand and sign an Acceptable Use Guideline form prior to using any equipment or the Internet within school

Online safety in community activities and after-school clubs

- When our school hires out or lets school facilities/premises to organisations or individuals (e.g. community groups, sports associations and service provider to run community or extra-curricular activities), we ensure that appropriate arrangements are in place to keep children safe.
- We seek assurances that where services or activities are provided separately by another body (not under direct supervision or management of our school staff) there are appropriate safeguarding and child protection policies and procedures in place (including online safety) and will inspect these as necessary. This applies regardless of whether or not the children who are attending these services are on our school roll.
- Safeguarding arrangements are clearly detailed in any transfer of control agreement (i.e. lease or hire agreement).

Vulnerable Learners

- We recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENDCO.

Communication:
The Online Safety Policy and Acceptable Use Guidelines will be communicated in the following ways:

- Posted on the school website.
- Part of school induction pack for new staff.
- Acceptable Use Guidelines to be issued to new school members on entry to the school
- Staff will read and sign the Code of Conduct for IT and Computing. This will be kept in their personnel file.

Handling complaints:
The school will take all reasonable precautions to ensure online safety. However, it is important to recognise that no system is 100% effective. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Infringements are dealt with in line with the sanctions and rewards system for children and misconduct policy for staff.

- Class Teachers act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The Online Safety policy and Acceptable Use Guidelines is referenced from within other school policies: Computing policy statement, Safeguarding policy, Anti-Bullying and Behaviour policy, Personal, Social, Health Education and Citizenship policies.

- The school has a Digital Leader who will be responsible for document ownership, review and updates.

- The online safety policy and acceptable use guidelines will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school

- The online safety policy and acceptable use guidelines has been written by a Designated Safeguarding Lead (DSL) and is current and appropriate for its intended audience and purpose.

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as parents' forum. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

Staff and governor training
This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program; through the use of annual updates/ termly staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety and Acceptable Use and Safeguarding Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Guidelines to new parents, to ensure that principles of online safe behaviour are made clear
    - Information on the school web site;
    - Regular updates on the Newsletter

- A termly Digital Bulletin explicitly for Online safety updates.
- Providing them with information about our approach to filtering and monitoring as well as information about the types of things that children will be doing online.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT systems in accordance with the relevant Acceptable Use Guidelines which they will be expected to sign before being given access to school systems. (At KS1 the parents/carers sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and Acceptable Use Guidelines covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the school's Online Safety Policy and Acceptable Use Guidelines and using the school IT systems accordingly.

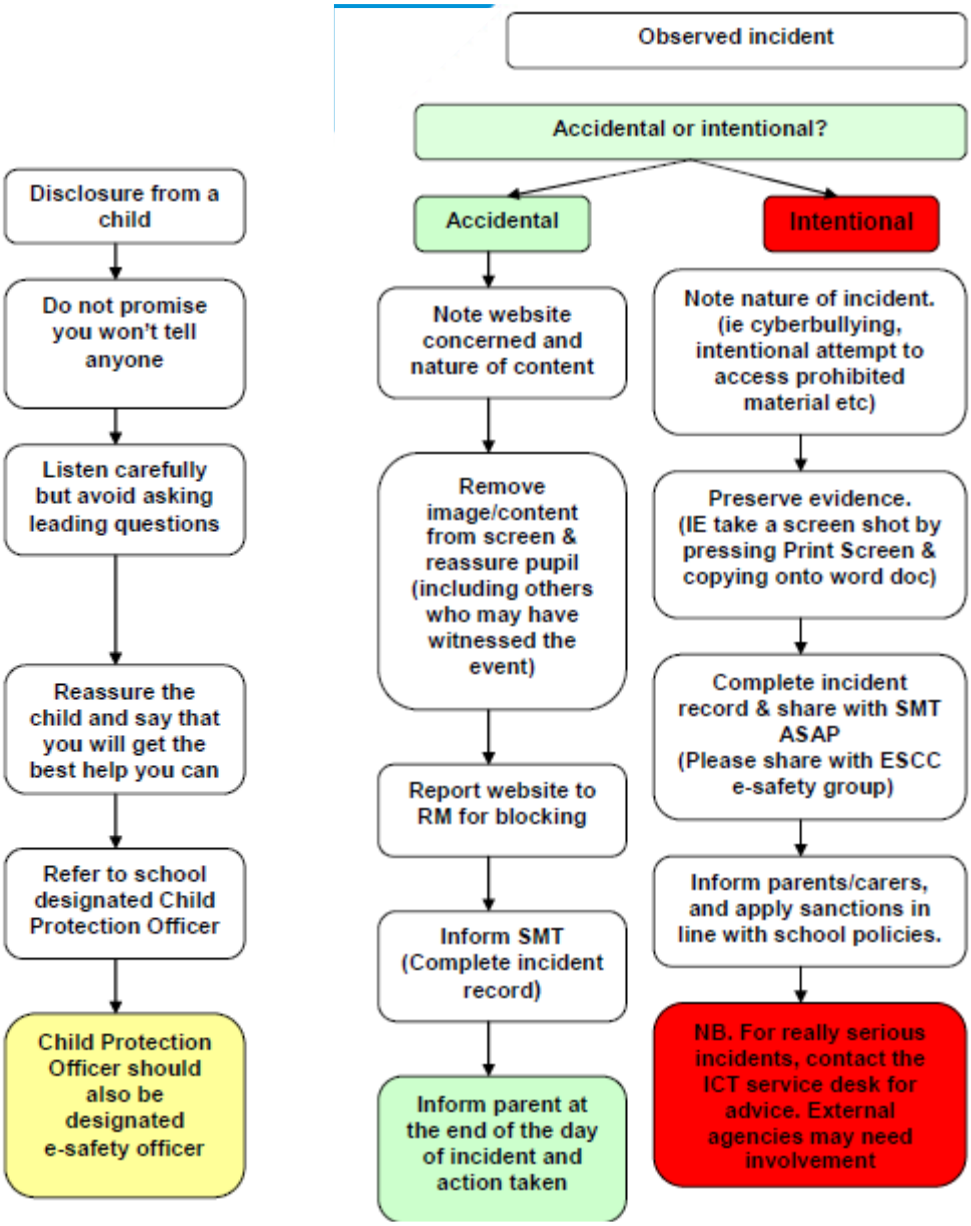
Pupils

- Should have a good understanding of what to do if they encounter age inappropriate material or material which makes them uncomfortable.

Families

- Should read and understand the online safety acceptable use guidelines for children and parents at time of their child's entry to the school as part of the new entrants pack.

Incident Management
Follows ESCC guidelines:



Managing the IT infrastructure

IT infrastructure management is undertaken by 'Schools IT' provided by East Sussex County Council with whom there is a service level agreement. Ashdown Primary School expects Schools IT to:

- Use ESCC approved systems such as S2S or secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Work in partnership with the local authority to ensure any concerns about the system are communicated so that systems remain robust and protect children;
- Inform all users that Internet use is monitored;
- Inform staff and students that that they must report any failure of the filtering systems directly to the IT Schools using the desktop service.
- Provide advice and information on reporting offensive materials, abuse/ bullying to the headteacher.
- Use individual, audited log-ins for all users;
- Use guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensure the Systems is compliant with DFE and ESCC requirements.
- Store of all data within the school in such a way to conform with UK/EU data protection requirements.

To ensure the network is used safely, the school:

- Requires staff to preview websites before use [where not previously viewed or cached] and; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google Safe Search or Kiddle. Children must use this rather than straight Google.
- Staff access to Arbor is controlled through a separate username and password for data security purposes;
- Currently pupils only have a class log-in and are not required to use an individual username and password.
- All pupils, where appropriate, have their own unique username and password which give them access to online curriculum resources e.g., Times Tables Rockstars, Purple Mash
- At present children do not have email access.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Makes clear that staff are responsible for ensuring that any computer, laptop or camera loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs. Staff are expected to connect all equipment to the network at least weekly so that updates are made.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support.
- Ensures that all pupil level data or personal data sent over the Internet uses the s2S website.
- Requires all adult to lock screens when leaving them unattended.

E-mail

This school

- Provides staff with an email account for their professional use only.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@ashdown.e-sussex.sch.uk (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- We do not send pupil level or personal data via email.

Pupils:

- Students do not have email access at present
- Staff and pupils may only communicate with each other electronically through the communication function on “purple mash”.

School website

- The Executive Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@ashdown.e-sussex.sch.uk Home information or individual e-mail identities will not be published;
- Photographs of children published on the web do not have names attached;
- We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website;

Social networking

- Social networking sites are filtered and not available to staff or students via the school network.
- The school social media accounts are only operated and accessed by the office and admin staff.

  https://www.facebook.com/friendsofashdownprimaryschool/

  https://twitter.com/AshdownPrimary

  https://instagram.com/foaps_pta?igshid=OGQ5ZDc2ODk2ZA==
- Schools have a vital role to play in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse.
- No reference should be made by staff in personal social media to students, pupils, parents, carers or other school staff, even between social networking ‘friends’.
- Staff must not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority. Any opinions or conduct that the Headteacher deems to have brought the school into disrepute will be dealt with using the staff disciplinary policy.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff must inform their line manager, the DSL (or deputies) and/or the headteacher/manager of any concerns, such as criticism, inappropriate content or contact from learners.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data security: Management Information System access and Data transfer
Strategic and operational practices

At this school:

- The Executive Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed
    - staff,
    - governors,
    - pupils
    - parents

  This makes clear staff's responsibilities with regard to data security, passwords and access.
- We insist that restricted material must not be taken of site.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Equipment and Digital Content

Students' use of personal devices

- The School strongly insists that student mobile phones should not be brought into school.
- The School accepts that there may be particular short term circumstances in which a parent wishes their child to have a mobile phone for their own safety. This should be switched off and handed to the office at the beginning of the day and collected on the way out.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers only.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use the school phone.

Staff use of personal devices

- Staff mobile phones should be on silent during the school day and left in a secure location (eg cupboard or desk drawer). Bluetooth security settings should be 'not visible'.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless it is an emergency. In the first instance staff should call the school first if practical.
- Staff should not use mobile phones to contact with students, parents or carers – landlines are available. The only school mobile phone is the one used by Extended After School Club. Please see the educational visits policy for use of mobile phones on trips.

- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use their own portable devices for taking pictures or video.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught that they should not post images or videos of others without their permission.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency (currently schools IT). This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies (currently schools IT) who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Ashdown
Primary School

Staff Code of Conduct for IT & Computing – to be signed annually.

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's online safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Digital Leader, the Designated safeguarding Lead or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for IT.

Signed:

Name: Date:

Ashdown
Primary School

Children Acceptable Use Guideline form

I understand that the following guidelines will help keep me safe and happy online:

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my personal school usernames and passwords safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, photos).
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to an adult in school or at home.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission of a member of staff to do so.
- I will not use the school systems or devices for on-line gaming or video broadcasting, unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I have read and understand the above guidelines are for when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. tablet, eBook, USB devices, cameras etc…
- I use my own equipment out of the school in a way that is related to me being a member of this school (e.g. communicating with other members of the school, accessing school email, website etc...)

Ashdown
Primary School

Family Acceptable Use Guideline Form

Parents and families are requested to read the information below to understand the school's Acceptable Use Guidelines.

- I know that my son / daughter has understood the Acceptable Use Guidelines and has received, or will 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 understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Guidelines.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.
- I will read and adopt the protocols outlined by the school prior to any video calls (Zoom, Microsoft Teams etc).

Online Safety for Children and Parents

Ashdown Primary School's Acceptable Use Guidelines - A Quick Guide

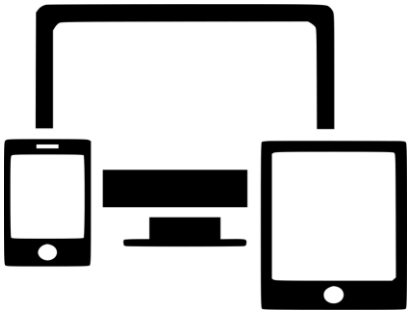
Must dos!

- Keep my personal school usernames and passwords safe and secure. Do not share these details!
- Be aware of "stranger danger" when online.
- Do not share personal information about myself or others online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, photos).
- Immediately report anything that makes me feel uncomfortable or that I know is wrong when I see it on-line to an adult in school or at home.

Remember to…

- Act as I expect others to act toward me.
- Respect others' work and property.
- Be polite and responsible when I communicate with others.
- Not take or distribute images of anyone without their permission.

.



Remember that…

- School can monitor my activity on school devices.
- School systems and devices are intended for educational use.
- School systems or devices are not for on-line gaming or video broadcasting, unless I have permission of a member of staff to do so.

Things for my parents to remember!

- My son/daughter has understood these guidelines, or will receive, online safety education to help them understand.
- The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I know that school will contact me if they have concerns about any possible breaches of these guidelines.
- Encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.
- Read and adopt the protocols outlined by the school prior to any video calls with school staff (e.g. parents evening on Zoom).

Please also refer to:

- Security policy
- Data protection policy
- Staff code of conduct
- Child protection and safeguarding policy