E-Safety Policy

Governor approval	Next review	Responsible Person
May 2021	As required	Computing Subject Leader

Policy Overview

Purpose

It is our duty at Ashdene to ensure that every child is safe. This policy document is drawn up to protect all parties – the children, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. This policy should be read in conjunction with the school's safeguarding policy.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Ashdene Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the pupils and staff.
- Assist school staff working with pupils to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- 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 pupils.

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

- Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gaming, body image)
- Copyright (little care or consideration for intellectual property and ownership)

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- Online abuse Protecting children from online abuse | NSPCC Learning
- Bullying Protecting children from bullying and cyberbullying | NSPCC Learning
- Child protection Child protection system in the UK | NSPCC Learning

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however it can also present risks and challenges.
- We have a duty to ensure that all members of the Ashdene community are protected from potential harm online.
- We have a responsibility to help keep children safe online, whether or not they are using Ashdene's network and devices.
- All children have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, their parents, carers and other agencies is essential in promoting their welfare and in helping children to be responsible in their approach to online safety.

Strategies used by Ashdene to keep children safe online

We will seek to keep children and young people safe by:

- Providing clear and specific directions to staff on how to behave online through our staff code of conduct.
- Supporting and encouraging children at Ashdene to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- Supporting and encouraging parents and carers to do what they can to keep their children safe online.
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child.
- Reviewing and updating the security of our information systems regularly.
- Ensuring that user names, logins, email accounts and passwords are used effectively.
- Ensuring personal information about the adults and children at Ashdene Primary School is held securely and shared only as appropriate
- Ensuring that images of children are used only after written permission has been obtained from parents/carers, and only for the purpose for which consent has been given.
- Providing supervision, support and training for staff about online safety.
- Offering support and guidance to parents on how to keep children safe online through parental workshops.
- Examining and risk assessing any social media platforms and new technologies before they are used by the school.
- Ensuring a clear, progressive online safety education programme is part of our Jigsaw PSHE curriculum and our Computing curriculum.
- Ensuring there is an educational filter on the server to block inappropriate content.

Expected conduct

At Ashdene, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements.
- Are aware that use of all school owned devices is monitored.
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences.
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practice when using digital technologies in and out of school.
- Know and understand school policies on the use of mobile and hand held devices including cameras.
- School owned devices are the only devices permitted for use during lesson time.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. This includes school-assigned and personal devices.

Staff:

- Know to be vigilant in the supervision of children at all times.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open internet searching is required with younger pupils.
- Staff have their own unique usernames and passwords and know they must always keep their passwords private.
- Staff know to log out or lock devices when not in use.
- Staff have their own email account that is for professional use only.
- Follow the school's social media policy, ensuring that no reference is made to the school on personal accounts.
- Personal devices should be turned off or put on silent. These are not permitted for use in the presence of children.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Staff follow the school's data protection policy for use of digital photographs and videos – permission from a parent carer must be given before images of children are shared online. These can only be shared for the purpose given. Pupils must not be identified in any images shared online.

Parents/Carers:

- Should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.
- Should know that only pupils in year 6 are permitted to bring their own mobile phone into school and should only do this if they have permission to make their own way to and from school. All personal pupil mobile devices are stored in the teacher's desk during the day. School will not accept responsibility for the loss, theft or damage of any mobile phone brought into school.

Managing incidents

Incident management

At Ashdene:

- All members of school staff are encouraged to be vigilant and to report any incident immediately to a member of the senior leadership team. Where the incident is a safeguarding matter, this should be reported to the Designated Safeguarding Lead.
- Following an incident, the appropriate behaviour, safeguarding or anti-bullying policy will then be followed.
- Support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school.
- Incidents are recorded using the school's CPOMs system where appropriate.
- Following an incident, parents/carers will be informed.
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

If online abuse occurs, we will respond to it by:

- Following the school's safeguarding policy and procedures for responding to abuse (including online abuse).
- Informing the school's Designated Safeguarding Lead and recording all incident on CPOMs.
- Providing support and training for all staff on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our school as a whole into account.
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Related policies and procedures

Our E-safety policy should be read in conjunction with our school policies for:

- Child protection and Safeguarding policy
- Behaviour Policy
- Managing allegations against staff and volunteers
- Staff code of conduct
- Anti-bullying policy
- Data protection policy
- Social media policy

NSPCC Helpline 0808 800 5000