At Ashfield Valley we care for and value every child in a nurturing, inclusive environment.

All members of our school community will work hard to ensure that every pupil achieves their full potential and has the opportunity to shine.

E-Safety Policy

Reviewed: September 2022

Date of next review: September 2023

1. INTRODUCTION AND OVERVIEW

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Ashfield Valley Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Ashfield Valley 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/or codes of practice relevant to responsible use of the Internet 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.
- Hate sites.
- Extremism exposure.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Sexual abuse. This can take place online, and technology can be used to facilitate offline abuse (Keeping Children Safe in Education, 2020).
- Sexual Harassment. Including non-consensual sharing of sexual images and videos, sexualised online bullying, unwanted sexual comments and messages, including on social media; sexual exploitation; coercion and threats and upskirting (KCSIE, 2020).
- Cyber-bullying in all forms. This can take place wholly online, or technology may be used to facilitate offline abuse (Keeping Children Safe in Education, 2020).
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.
- CSE (Child Sexual Exploitation) and CCE (Child Criminal Exploitation)

Conduct

- Privacy issues, including disclosure of personal information.

- Digital footprint and online reputation.
- Mental Health and well-being (amount of time spent online Internet, impact of cyberbullying or gaming).
- Sexting (sending and receiving of personal intimate content / images).

2. SCOPE

This policy applies to all members of the Ashfield Valley Primary community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.
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 cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of school, but are linked to school.
School leaders will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be stored on network location.
- Policy to be part of school induction pack for new staff.
- Staff to sign acceptable use agreement annually.
- Acceptable use agreements to be held in personnel files.

Handling complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.
Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by the Welfare Team / Senior Leaders / Headteacher
- Informing parents or carers
- Temporary removal of Internet or computer access for a period
- Referral to LA / Police or other authorities.

Any complaint about staff and student 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 child protection procedures.

Review and Monitoring

- The school has an IT lead (Mrs Nisar) who will be responsible for document ownership, review and updates.

- The e-safety policy will be reviewed annually or when any significant changes occur about the technologies in use within the school.

3. EDUCATION AND CURRICULUM

Pupil e-safety curriculum

Ashfield Valley Primary School has a clear, progressive e-safety education programme as part of both the pastoral system and curriculum. It covers a range of skills and behaviours including:

- To STOP and THINK before you CLICK
- To follow the SMART rules for staying safe online
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To understand how child on child abuse can take place online, including sexual harassment (KCSIE, 2022).
- To recognise the impact of technology on mental health and wellbeing.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Child Line.
- Careful planning of internet use to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff training

Ashfield Valley Primary School will:

- Provide, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies
- Ensure that all staff have general safeguarding training yearly which covers elements of e-safety.

Parent awareness and training

Ashfield Valley Primary School will:

- Use information leaflets, Internet Safety Day, school newsletters, and the school web site to raise awareness of e-safety.
- Provide suggestions for safe Internet use at home.
- Provide information about national support sites for parents.

4. EXPECTED CONDUCT AND KEY RESPONSIBILITIES

In this school, all users:

- Are responsible for using the school IT systems in accordance with school procedures.
- 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 E-Safety Policy 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.

Roles and Responsibilities:	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision. • To ensure the school uses a, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.

	• To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. IT Lead).
IT lead (including role of E-safety co-ordinator)	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with school ICT technical staff. • Oversees the delivery of the e-safety element of the Computing curriculum • Alerts the HT and SBM of any e-safety related issues that arise • Keeps up to date with current practice and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
Parents/carers	• To support the school in promoting e-safety. • To consult with the school if they have any concerns about their children's use of technology.

5. MANAGING THE INFRASTRUCTURE

Internet access, security (virus protection) and filtering

Ashfield Valley Primary School:

- Has a secured broadband connection and filtering system that blocks sites that fall into unsuitable categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Only unblocks other external social networking sites for specific purposes.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that all computer use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
- Requires all users to always log off when they have finished working or lock their computers when leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to re-enter the network. Any flaws in this must be reported.
- Has set-up the network so that users cannot download executable files / programmes.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password

School Website

- The school website is managed by the IT lead (Mrs Nisar) and the Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school website complies with the statutory DfE guidelines for publications and reviewed on a regular basis.
  Photographs published on the web do not have full names attached;

Social networking

- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- School staff will ensure that in private use:
    - No reference should be made in social media to pupils, parents / carers 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 school or local authority

Video Conferencing /Home Learning

- Only uses approved or checked webcam sites;

6. EQUIPMENT AND DIGITAL CONTENT

- Personal mobile phones and mobile devices
    - Please see mobile phone policy

Digital images and video

- 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 or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school website, 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 about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.