# Ashfield Primary School

# E-SAFETY AND ACCEPTABLE USE POLICY

## Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet-based technologies that children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms
- Email and Instant Messaging - (Instagram, Whatsapp, Snapchat, Twitter etc)
- Chat Rooms and Social Networking sites - (Facebook etc)
- Blogs and Wikis
- Podcasting
- Video Broadcasting – (Youtube, Facebook etc)
- Music Downloading – (Spotify, Apple Music etc)
- Online gaming, including web-linked gaming on console games
- Mobile / Smart phones with text, video and web functionality
- Other mobile devices with web functionality (including tablets and iPads)
- File/photo sharing (Snapchat, Instagram, Pinterest)

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Ashfield Primary School (APS), we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school; (including existing ones such as PCs, laptops, whiteboards, digital video equipment, cameras; and possible future resources including tablets, webcams, voting systems, etc) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

# CONTENTS

## 7. APPENDICES

*** Rules for Acceptable Internet Use – Pupil Version**

*** Rules for Acceptable Internet Use – Staff Version**

*** Updated image permission form**

# SECTION ONE: Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The ICT Leader will act as an eSafety co-ordinator whose role is to keep abreast of current issues and guidance through organisations such as Leeds LEA, CEOP (Child Exploitation and Online Protection) and Childnet. Other staff members have the responsibility for monitoring the e-safety of the pupils that they work with, and will inform the eSafety co-ordinator or Headteacher should any issues or concerns arise which may put children at risk.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

## a) eSafety Skills Development for Staff

- Staff should receive regular information and training on eSafety issues in the form of staff meetings and CPD, as appropriate.
- New staff will receive information on the school's acceptable use policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate eSafety activities and awareness within the direct teaching of Computing and ICT, and within other curriculum areas that involve the use of ICT.

## a) Managing eSafety Messages in the Curriculum

- At APS, we endeavour to embed clear eSafety messages across the curriculum whenever the internet and related technologies are used.
- eSafety guidance should be given to the pupils on a regular and meaningful basis, and embedded within ICT opportunities throughout the curriculum.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils, (particularly those higher up in school) should be made aware of the relevant legislation when using the internet; such as data protection and intellectual property which may limit what they want to do, but also serves to protect them.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Relevant aspects of the e-safety policy will be explored with the pupils at the start of each school year, and throughout the year as appropriate. Other opportunities may be used (such as *'e-safety week'*) to focus on children's safety outside the school.
- E-safety posters are prominently displayed around school and in clasrooms
- Parents are provided with safety information via the school newsletter and school website, e.g inappropriate websites, safe management of computers in the home, links to safety advice as and when needs arise. The school website includes 'safe' links for pupils when researching most topics.

## SECTION TWO : SECURITY

### a) Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Staff should be aware of their responsibility when accessing school data. The level of access is determined by the Headteacher. Pupil data should only be accessed and used on school computers or laptops.

### b) Managing the Internet

The internet is an open communication medium, available to all, and at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. In school, all use of the internet and its associated resources is logged and any breaches are flagged via email to the computing lead and headteacher. Whenever any inappropriate use is detected it can be followed up.

- The school maintains that students will have supervised access to internet resources through the school's fixed and mobile internet technology.
- Staff should preview any recommended sites before use.
- If internet research is set for homework, specific sites can be suggested that have previously been checked by the teacher. Such sites can be set up beforehand to be linked directly from the School Website if required. It is however advised that parents still recheck these sites and supervise this work, as well as any further research due to the flexible nature of web publishing.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

### c) Infrastucture

- School internet access is controlled through the school's web filtering service.
- Staff and pupils are aware that school based email (Gmail) and internet activity can be monitored and explored further if required. Consequences of misuse will be shared with children, and strict expectations will be upheld.
- If staff or pupils discover an unsuitable site, the web page should be closed on screen and the incident reported immediately to the teacher or the eSafety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines. Users should not intentionally prevent updates of software from running on machines.
- Pupils and Staff using personal removable media (memory sticks, removable drives etc) are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the *class teacher* for a safety check, using the school's virus scan first. An alternative method is available to staff and pupils in KS2 through the use of Chrome Drive (or similar resource) as a secure method of storage and retrieval of documents and files.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the eSafety co-ordinator / technician.
- If there are any issues related to viruses or anti-virus software, the Computing Leader should be informed immediately.

## d) Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Pupils are encouraged to keep their passwords secret and not to share with others, particularly their friends.

- All users should read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy.
- Users are provided with individual Google Classroom usernames. In upper KS2 they are also expected to use a personal password and keep it private. Pupils may also have individual passwords for online learning resources, such as TT Rockstars which also should be secure.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, that belong to their peers, teachers or others, without the express permission from those involved, and even then, this should be discouraged.
- If staff or pupils think that their password may have been compromised, this should be reported to the Computing Leader as soon as possible.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended for long periods without logging off or securing them first.

## SECTION THREE: TECHNOLOGIES AND COMMUNICATION

## a) Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to make or exceed age expected progress in ICT, pupils must have experienced sending and receiving emails. For security purposes in the context of school, email should not be considered private and Gmail accounts may be monitored for content within the school's Acceptable Use Policy.

- The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. Staff are requested not to use the school email for personal communication.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- E-mail sent to an external organisation should be written and checked carefully before sending, in the same way as a letter may be written on school headed paper.
- Pupils are introduced to email as part of the Computing Schemes of Work.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Virus checking of attachments is also necessary to protect school systems.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail or online communication.

## b) Using Resources from the Internet

We believe that, in order to access the internet effectively, it is important for pupils to develop an understanding of the nature of the web and the resources within it. In particular, they should know that, unlike a 'fixed' resource such as a book, many of the resources available on the internet can be intended for an adult audience, may not be properly audited, edited, and may be subject to copyright.

- Pupils will be taught to expect a much wider range of content, both in level and in audience, than is found in a library or on TV.
- Teachers will encourage pupils to validate information wherever possible, in terms of its authors, publishing date and neutrality, and make them aware that not all resources are reliable.
- When using resources from the internet, pupils will be taught to observe copyright.

## c) Web 2 Technologies

'Web 2' technologies include the interactive use of resources that are primarily web-based, including social networking sites, (eg *Facebook. Twitter, Instagram/Snapchat, Whatsapp* etc) Cloud computing and increasingly use of Apps on mobile systems. If used responsibly, both outside and within an educational context, these can provide easy to use, creative, collaborative and free facilities. It is important however to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism within such media. In an increasingly technological world, it is not always possible to restrict pupils' access to such e-Safety dangers. To this end, we therefore encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such sites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are, no matter how subtle they may seem.
- Our pupils should be advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils should be encouraged to be wary about publishing specific and detailed private thoughts online, and advised to consider others' personal rights when publishing materials that contain data that is not strictly their own, for example group images.
- Our pupils are asked to report any incidents of cyber-bullying to parents/carers and the school.
- Staff may only create blogs, wikis or other Web 2 spaces in order to communicate with pupils using systems approved by the Headteacher.

## d) Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, iPads/tablets, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative device with internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Personal Mobile devices (including phones)**

- The school allows staff to bring in personal mobile phones and devices for their own use. Members of staff should not contact a pupil or parent/carer using their personal device.
- Pupils should not bring personal mobile devices/phones to school, unless previously agreed with the Headteacher. If devices are accidentally brought into school, these must be handed in to the office.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages between **any** member of the school community is not allowed using any media. Staff should be particularly aware of private and professional concerns when adding 'friends' to sites such as Facebook. For their own professional security it is not recommended that staff accept 'friend' requests from current or past pupils unless they are part of wider family or friendship circles outside of the school.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

# SECTION FOUR: SAFE USE OF IMAGES

## Taking of Images and Video

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- The school permits the appropriate taking of images by staff and pupils with school equipment. Written consent of parents/carers for this is asked for when a child first enters school. This should be kept in the child's file, and a list kept by the class teacher of any children who do not have consent.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others.

## a) Publishing Pupil's Images and Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school website
- on the school's MIS
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where

consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

## b) Storage of Images

- Images/videos of children are stored on the school's network and should be deleted when those children leave the school. It is the duty of staff members who take or store the photos to ensure that this occurs.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

## c) Webcams/Video Conferencing

- Webcams in school are used for specific learning purposes, and should only be used in adult-led teaching situations or training purposes or Zoom / Teams calls.
- Misuse of a webcam by any member of the school community will result in sanctions as part of the school behaviour policy.
- Permission should be sought from parents and carers if their children are involved in video conferences.
- All pupils should be supervised by a member of staff when video conferencing.
-

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

# SECTION FIVE: ESAFETY MANAGEMENT

Whilst the school puts into place systems to manage and monitor access to the internet, the international and ever-changing scale of the web means that it is not always possible to guarantee that particular material will never appear on a computer screen. Neither the school nor the LA can accept liability for material accessed, or any consequences thereof.

An important element of our Acceptable Use policy is that pupils will be encouraged to tell a member of staff **immediately** if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incident involving children will be taken by the ICT Leader and Child Protection Officer in consultation with the Headteacher and the class teacher. All teaching staff will be made aware of the incident in a staff briefing if appropriate.

- If one or more pupils discover (view) inappropriate material, our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action that the school has taken. The school will aim to work with the parents/carers to resolve any issues.

- If staff or pupils discover unsuitable sites, the Computing Leader and the Safeguarding Lead will be informed. The Computing Leader will take appropriate action, which may include reporting the URL address to the appropriate authorities.

## a) Misuse and Infringements

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by following the Acceptable Use Policy. If pupils abuse the privileges of access to the internet or use of email facilities, then sanctions consistent with the school's Behaviour Policy will be applied. This may involve informing parents or carers. Teachers may also consider whether access to the internet may be denied for a period.

## b) Complaints

Complaints relating to eSafety should be made to the class teacher or Computing Leader in the first instance, if the complaint is not dealt with satisfactorily then a further complaint should be made to the Headteacher. Incidents should be logged, and kept in a central location.

## c) Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Computing Leader/Headteacher.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see attached flowchart.)

# SECTION 6: Equal Opportunities

## a) Pupils with Additional Needs

The school endeavours to create a consistent message with families for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.
However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

## b) Parental Involvement

We believe that it is essential for families to be fully involved with promoting eSafety both in and outside of school. We aim to consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website/Facebook page)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website postings
    - Newsletter items

This policy should be reviewed regularly, and take into account the ever-changing nature of the technologies involved.

# SECTION SEVEN: APPENDICES

## Ashfield Primary School

## RULES FOR ACCEPTABLE INTERNET USE – PUPIL VERSION

The school has a range of computers and other devices that enable users to access the internet to support their learning. These rules are designed to keep us safe, and will help us to be fair to others.

### Using Computers, Laptops or Similar Devices

- I will only access the network system with permission from an adult in school.
- I will not access other people's files without their permission.
- I will not bring in storage drives (memory sticks, portable hard drives etc) from outside school and try to use them on school machines without asking permission.
- I will not print at school unless I have permission from an adult in school, and will not print more than once at a time if the print does not work.
- I will only use school machines for school work or homework, unless I have permission from my teacher.
- I will not download any software onto the school system without permission from an adult.

### Using the Internet

- I should ask permission from an adult in school before using the internet.
- I will report any unpleasant material to my teacher **immediately** because this will help protect other people as well as myself
- I understand that the school may check my computer files and may monitor the internet sites that I use in school.

- I will not deliberately access sites that are not allowed in school, or that I know may be unsuitable.
- I know not to click on 'pop-up' adverts, for example '*You have Won…*'
- I will not give my full name, home address or telephone number to anyone when filling in forms on the internet. I will not speak to people that I do not know online unless a teacher has already organised this.

## Using Email or Other E-communication

- I will ask permission from a teacher before using email.
- I will immediately report any unpleasant messages sent to me, because this will help to protect other pupils and myself.
- I understand that messages that I receive or send in school may be read and checked by adults. Private messages should be sent outside of school using a different email account.
- I am responsible for my own email account. The messages that I send will be polite and responsible.
- I will not share my password details with others, and will let my teacher know immediately if I believe that someone else is misusing my account.
- I will only email people that my teacher has approved.
- I will not share my personal details using email, chat to or arrange to meet anyone that I do not know via email.

## Mobile Technology

- I will not bring my mobile phone or mobile device to school, unless agreed beforehand with a teacher.
- If I accidentally bring in my device, I will take it to the school office to keep it safe.
- The school is not responsible for any device that I bring into school, should it get lost or stolen.
- I will not use my mobile phone or any other technology to bully, cause offence or damage to our school, its pupils and staff.
- I will immediately report any inappropriate messages to a member of staff.

I agree to the above Acceptable Internet Rules in order to keep myself and others safe.

Name_____ Signed_____
Date_____

# Ashfield Primary School

## ACCEPTABLE INTERNET USE STATEMENT – STAFF VERSION

### Within the School and the Network

The computer networks are owned by the school and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Acceptable Use Policy has been drawn up to protect all parties – the children, the staff and the school.
The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.
Staff requesting internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Headteacher.

### Using the Network

- All internet activity should be appropriate to staff professional activity or the children's education.
- Access to the network and internet should only be made via the authorised account and password, which should not be made available to any other person (staff member or pupils)
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware of software without permission of the Computing Leader

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher. Images/recordings will only captured on school equipment.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to Headteacher.

## Using Email or Other E-communication

- Users are responsible for all emails sent and for contacts made that may result in email being received.
- The school's email system should only be used for professional purposes. Personal messages should be sent using a private account from another provider.
- Use for email for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Emails must not be amended without the original senders permission prior to forwarding

## Outside School

The Computing Leader will forward information and advice relating to safe keeping when using the internet, emails and mobile technology on a personal level.
The school understands that it cannot dictate what staff do in their personal time, but it will endeavour to give them the information to ensure that everyone acts safely and professionally.
Staff are advised professionally however to ensure that their online activity, both in school **and** outside school, will not bring their professional role into disrepute.

---

**Please complete the following:**

- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

- I agree to follow the guidelines for computer and Internet use as outlined above and in the school's Internet policy.

Name_____ Signed_____
Date_____

## PERMISSION FOR IMAGE USE ON THE SCHOOL WEBSITE/Facebook page

Dear Parent(s)/ Carer,

As you may be aware, our school has a website and Facebook page in operation, available at the following address: www.ashfieldprimary.co.uk . We feel that this enables parents and families to access information more easily and to become more involved in the life of their children at school.

As technology has advanced, we now use a lot of digital photography and video making as part of the school curriculum. In order to share this learning with you, we would like to be able to use images (including video) of our children and staff on our website.

Where permission is given for images of children to be used, we will undertake to ensure that children will not be identifiable by name. Where permission is not given to use images, we will ensure that they do not miss out on any opportunities as a result of this.

We would be grateful if you can fully complete and return this updated permission form indicating your preferences. We hope that you feel able to support us in this endeavour and we can assure you that the utmost care will be taken to ensure the safety of all. Information will be used sensitively.

If you would like to discuss this matter, please do not hesitate to contact us at the school.

✂----------

Child's name:_____ Current year group _____

Please delete as appropriate:

1. I do/do not give my permission for my child's (unnamed) photograph to be used on the school website.

2. I do/do not give my permission for video footage featuring my child to be used on the school website.

3. I do/do not give my permission for my child's work to appear on the school website, when it does not contain an image of their face. (audio broadcasts, distance shots, images of art/design projects etc)

Parent/Carer
Signature_____Date_____

Class …… Date ……

**Agreed by Governing Body of Ashfield Primary School 4/12/2024**
**Related policies:**

- **Complaints**
- **Safeguarding and Child Protection**
- **Computing**
- **PSHE**

**Next Review date: December 2026**