Alumwell Infant School

Learn, Grow and Achieve

On-line Safety Policy

Signed by The Chair of The Governing Board: **Signed copy available in school office**	
Date policy ratified by governing body:	**November 2023**
Date of policy's review:	**November 2025**
Review Schedule:	**Bi - Annual**
Policy Author:	**AIS** **Updated September 2025**

Contents

Introduction

At Alumwell Infant School, we are very aware that the modern technological world means that young children are having increasingly easier and more frequent access to the internet, through different sources such as; games consoles, mobile devices, tablet devices etc.

Whilst we believe this can be positive in developing and enhancing pupils' development and learning, we are also concerned about the risks this can bring;

Risks and potential dangers of using the internet;

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including people they don't know and trust in the real world
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

Aims

Through this policy, the staff at Alumwell Infant School strive to:

- keep pupils safe when using online technology in school
- educate pupils of the potential risks they can face when online, outside of school and how to deal with such situations
- ensure staff use online resources responsibly and professionally

Roles and Responsibilities

Responsibilities are delegated amongst staff members to ensure that online safety is monitored and taught appropriately. These roles and responsibilities are outlined in conjunction with the school's Safeguarding and Child Protection policies.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

A member of the Governing Board has taken on the role of Online Safety Governor who is Mrs H. Canlett. The role of the Online Safety

Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs (safeguarding)
- reporting to relevant Governors
- Receive annual training for online safety (this can be completed in a number of ways including face-to-face and online courses).
- Review the risk profile of the school and ensure that the filtering and monitoring solutions meet the needs of this risk profile

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Head teacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring of the school network by an external source (Walsall Online Monitoring service).
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Walsall Monitoring service via Smoothwall Monitor.
- The Head teacher will remain responsible for the filtering and monitoring solutions in order to protect users from seeing inappropriate content and behaving appropriately whilst on devices.

Online / IT Co-ordinator

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- meets regularly with Online Safety Governor to discuss current
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
- ensuring that Online safety is an integral part of the Computing curriculum in school
- delivering or facilitating training on Online safety to both staff and parent(s)/carer(s)

PSHE Co-ordinator

- Ensuring that Online safety is addressed through the PSHE curriculum in school

Network Manager/Technical staff

The Network Manager / Technical Staff / is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy/Guidance that may apply.
- that Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety 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 / internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher/ Senior Leader; Online Safety Coordinator for investigation/action/ sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher/ Senior Leader; Online Safety Coordinator for investigation/action/ sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they 'actively' monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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
- online bullying

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (see appendix l)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
- should 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

Parent(s) and Carer(s)

Parent(s)/Carer(s) play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.
Alumwell Infant School will take every opportunity to help parents understand these issues through newsletters, letters, website, parent workshops and information about national /local Online safety campaigns.
Parent(s) and carer(s) will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- online resources recommended by the school

Parent(s)/Carer(s) are asked to read information regarding online use in school and to discuss this with their child. They are then asked to sign a 'Pupil Acceptable Use Policy Agreement' with their child.

At this time parent(s) and Carer(s) are also asked to give their permission for their child to use the internet and technology equipment in school.

How is Online safety addressed in school?

We believe that the internet can be a very powerful tool to enhance our pupils' learning, however we are also aware of the dangers that it can pose. Pupils are encouraged to use the internet as a source of information as well as to access appropriate online resources to support learning.

The pupils are supervised at all times when using the internet in school. The school has a strong filtering system which on the whole, reliably denies access to unsuitable material on the internet.

Unfortunately, there may be incidents where staff or pupils access sites that are unsuitable. These incidents must be reported immediately to the safeguarding lead, a member of the SLT or the Computing co-ordinator so that they can inform the appropriate person at IT services.

Pupils are 'taught' Online safety through PSHE units of work as well as units of work in Computing using Purple Mash resources and Online safety lessons.

Pupils are taught:

- where and who to go to if they are worried or uncomfortable about content they have met online
- the importance of keeping personal information private
- to use online resources with adult permission and supervision, when inside and outside of school
- to be critically aware of the material they meet online-is everything on the internet true?

Education - Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring regulation of the children's on-line behaviours.

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website, Family sessions

Published Content – see GDPR Policy

Pupils' work is published onto the school's website as well as school literature.

Photographs and videos showing pupils will only be published on the school website/social media/local press, if parent(s)/carer(s) have given written permission on their child's contact form.

Looked After Children (LAC) will not have photographs published.

Staff use of Online Resources

Staff are encouraged to use the internet responsibly and professionally, when both in school and outside of school. All staff have to agree to and sign a 'Staff and Volunteer Acceptable Use Policy Agreement.' (See appendix 2).

Staff have been trained and advised to not disclose personal information or accept 'friend requests' from pupils or their parent(s)/carer(s) when using social networking sites, such as Facebook, X, WhatsApp etc.

Staff have their own school e-mail accounts and are encouraged to use these for professional activities only. They are advised to use the internet in school, for professional and school use only and not for personal activities; such as; online shopping.

Staff are encouraged not to take photographs or videos on their personal mobile devices, such as; mobile phones and tablet devices.

Staff devices are loaned by the school and are for professional use only.

Filtering of school internet

- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by using https://testfiltering.com. This is monitored every term by logging into different devices as different users and saving the results to the school network should anyone request to see these. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering for different access between pupils and staff

Reporting and Monitoring of Online Safety

Online safety procedures and the Online safety curriculum taught to pupils will be monitored and reviewed regularly in school, using tools such as the '360 degree safe- the Online safety self-review tool.' http://www.360safe.org.uk/

The school use an Online monitoring service (Walsall Online Monitoring using Smoothwall Monitor) to highlight any inappropriate online activity by both staff and pupil users within school.

This system generates an alert and a weekly report, which is analysed by a senior leader and any irregular or suspicious online activity, is investigated.

Smoothwall Monitor is used across the network in order to;

- Monitor inappropriate use of language
- Monitor internet usage including words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy (See Appendix)

Any identified incident is reported to Mrs Hammond (Head teacher) and Mr Evans (Deputy Head Teacher). In order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by a Local authority online safety advisor and reported via email.

A weekly email that gives an update on the number of users (people who log into devices), the number of devices that are being monitored and number of captures in the week. A monthly report is sent that includes details relating to school captures and incidents. This helps and supports us to identify the risk profile and look at patterns in the captures.

The monitoring software does not negate the need for staff to supervise pupils when using devices and it should be noted that it works on networked devices and chrome books but not IPads. IPad use should be fully supervised by staff and websites given to pupils in order to reduce the risk of coming across inappropriate content.

If any member of staff is concerned about an Online safety issue, (even if it is an incident that has taken place outside of school), they need to

inform the safeguarding lead, deputy head or a member of the Senior Leadership Team. The concern will be logged in the school's CPOMS (Child Protection Online Management System).

The issue will then be evaluated in conjunction with Safeguarding and Child Protection Policies, to ascertain how the concern will be dealt with and whether outside agencies need to be informed.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				*Pupils*				
Communication Technologies	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school		X			X				
Use of mobile phones in lessons	X				X				
Use of mobile phones in social time		X			X				
Taking photos on mobile phones	X				X				
Use of other mobile devices e.g. tablets,			X				X		
Use of personal email addresses in school, or on school network					X				

Use of school email for personal emails	X				X				
Use of messaging apps	X				X				
Use of social media	X				X				
Use of personal blogs	X				X				

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities, which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	

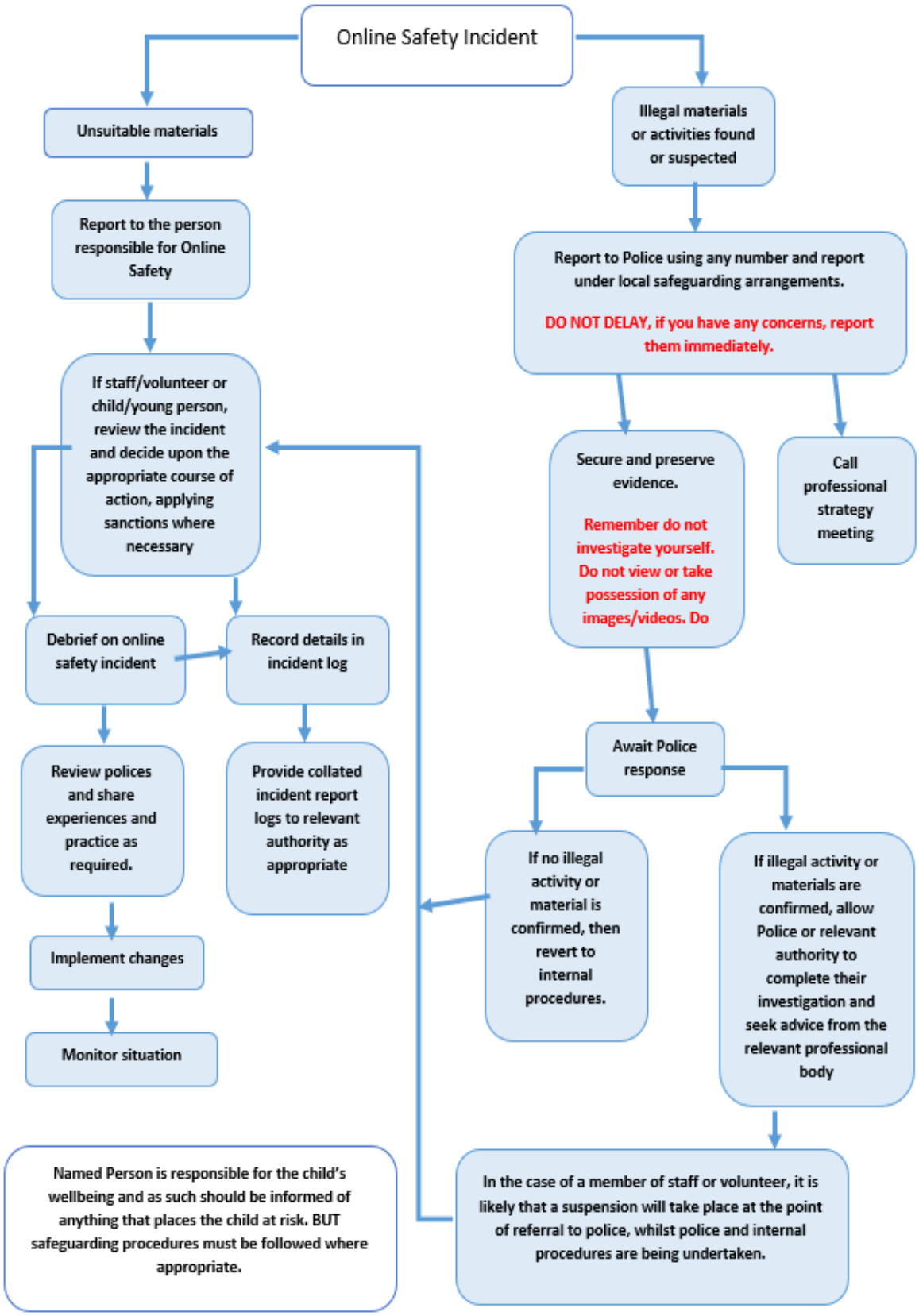
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright					X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X
Creating or propagating computer viruses or other harmful files					X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g.Youtube / TikTok		X			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

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


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection). Please notify the Online Monitoring Service too so alerts are not sent out regarding content looked at.
- Record the URL (website address) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or Involvement by Local Authority or national /local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.

Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. (Please do not shut down machines or log off)

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupils Incidents	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal	X	X		X	X	X	X
Unauthorised use of non-educational sites during lessons	X			X		X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X		X	X		X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X		X	X		X	X
Allowing others to access school network by sharing username and passwords	X		X	X	X	X	X
Attempting to access or accessing the school network, using another pupil's account	X			X	X	X	X

Attempting to access or accessing the school network, using the account of a member of staff	X			X	X	X	X
Corrupting or destroying the data of other users	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X			X	X	X	X

Staff Incidents	Refer to Headteacher	Refer to Governing	Refer to Police	Refer to Technical Support Staff for	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X		X	X
Inappropriate personal use of the internet / social media / personal email	X	X			X	
Unauthorised downloading or uploading of files	X				X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					
Deliberate actions to breach data protection or network security rules	X	X			X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X

Using personal email / social networking / instant messaging / text messaging to carry out digital communications with / pupils	X	X			X	X
Actions which could compromise the staff member's professional standing	X	X			X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X
Breaching copyright or licensing regulations	X					
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X

Appendix 1- Pupil Acceptable Use Policy Agreement

Pupil Acceptable Use Policy Agreement

At Alumwell Infant School we are very keen to develop your child to be a responsible user of the internet and ICT equipment. We believe that parent(s) and carer(s) have a vital role to play in this,

Please talk to your child about how to stay safe online and when using ICT equipment. A useful website to help you in this: www.thinkuknow.coeuk/

This is how we stay safe when we use computers and online material:

- I will ask a teacher or suitable adult if I want to use the computers
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong,
- I will tell a teacher or suitable adult if I see something that upsets or worries me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child) •.....

Signed (parent) •.....

Appendix 2- Staff and volunteer Acceptable Use Policy

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other Users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the pupils in my care in the safe use of ICT and embed e-safety In my work with pupils.

For my professional and personal safety:

- I understand that Alumwell Infant School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, school website etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are intended for educational Use and that I will only use the systems for such use
- I will not disclose my username or password to anyone else, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Alumwell Infant School's ICT systems:

- I will not access, copy, remove or otherwise alter any other users files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these

images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parent(s) / carer(s) using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Alumwell Infant School

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using Alumwell Infant School equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try/ to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Personal Data Policy (or other relevant policy).
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Alumwell Infant School:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name _____

Signed _____

Date _____