

Nether Alderley Primary School

e-Safeguarding Policy

Nether Alderley Primary School

e-Safeguarding Policy

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents .

E-Safeguarding underpins the principles for all use of technologies at Nether Alderley Primary School. We embrace the use of technology across the whole curriculum to enhance users' experiences and are committed to implementing robust and systematic procedures that help keep users safe from threats relating to electronic safeguarding. This policy will be reviewed on an annual basis or in response to an e-safeguarding incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

This policy is available for anybody to read on the school website; upon review all members of staff will sign to say that they have read and understood both the e-safeguarding policy and the staff e-safeguarding agreement. The pupils' e-safeguarding agreement will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Headteacher Name: Richard Craven Signed: _____

Chair of Governors: John Brooks Signed: _____

Review Date: November 2015 Next Review: November 2016

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safeguarding incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safeguarding incidents are appropriately dealt with and ensure the policy is effective in managing those incidents.

- The e-safeguarding governor is Mrs Nina Mowforth who has overall responsibility for the governance of e-safeguarding at the school and who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher / in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safeguarding within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safeguarding Officer, as indicated below.

The Headteacher will ensure that:

- E-Safeguarding training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safeguarding Officer has had appropriate CPD in order to undertake the day-to-day duties.
- All e-safeguarding incidents are dealt with promptly and appropriately.

e-Safeguarding Officer

The day-to-day duty of e-Safeguarding Officer is devolved to Andrew Brady.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on all e-safeguarding matters.
- Engage with parents and the school community on e-safeguarding matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safeguarding incident log (see Annex 1)**;** ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safeguarding measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- be aware of any reporting function with technical e-safeguarding measures, i.e. Internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

IT Technical Support Staff.

This policy also affects any technical staff that work in and on our school infrastructure and software.
(They must agree to it and sign it as if they are a member of staff)

Technical support staff (Fallibrooome support staff / Jigsaw 24 staff) are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows and Apple OSX / iOS updates are regularly monitored and devices updated as appropriate.
- Any e-safeguarding technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- Passwords are applied correctly to all users regardless of age.

All Staff

Staff will ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safeguarding incident is dealt with in line with this policy and the Safeguarding policy in school. Incidents are reported to the Headteacher and e-Safeguarding Officer (and an e-Safeguarding Incident report is written and put in the e-safeguarding incident log-held by the Headteacher), or in his absence to the Deputy Headteacher.
- The reporting flowcharts contained within this e-safety policy are fully understood (see Annex 2).

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the pupil e-safeguarding agreement (see Annex 3); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safeguarding is embedded into our curriculum with regular, planned and progressive lessons/opportunities for developing pupils' knowledge and skills along with any necessary and appropriate advice and guidance by staff. Similarly all pupils will be fully aware of their expected use of technologies through assemblies and eSafeguarding rules, which are displayed in every classroom. They are aware of what action to take should they be concerned whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and the school website, parents are kept up to date with new and emerging e-safeguarding risks.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will be asked to co-sign with their child the pupil's e-safety agreement.

Technology
Our school uses a range of devices including laptops, iPads, digital cameras and Apple Mac. In order to safeguard pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering
We use Cheshire East's IT services' filters to prevent unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The e-Safeguarding Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering
School emails are provided through a secure website using Microsoft Exchange which is provided, managed and supported by Cheshire East's ICT team. It prevents any infected emails being sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords
All staff and pupils will be unable to access any device(except the school iPads for pupils) without a unique username and password.

Anti-Virus
All capable devices will have anti-virus software. This software will be updated regularly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet
Use of the Internet in school is a privilege, not a right. Internet use will be granted:
to staff upon reading this e-safety policy and signing the staff e-safety agreement (see Annex 4); pupils and parents/ carers upon signing and returning their acceptance of the e-safety agreement (see Annex 3).

Pupils will be taught and shown through lessons and example good online activities and practices e.g. responsible use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development

Pupils will:

- Follow rules for Internet access; they are displayed in all classrooms.
- Understand the need for the pupil e-safeguarding agreement.
- Have equal access to use of the Internet in a safe and secure environment.
- Be taught about responsible use of the Internet, World Wide Web and e-mail.

All Staff will:

- Use their authorised account and have a password that should not be made available to any other person, except at the discretion of the head teacher.
- Ensure sites and materials accessed are appropriate to work in school.
- Not use own cameras or mobile devices for storing images from school.
- Be responsible for all e-mails sent and for contacts made that may result in e-mail being received.

- Maintain that the same professional levels of language and content are applied as for letters or other media, particularly as e-mail is often forwarded.
- Know that posting anonymous messages and forwarding chain letters is forbidden.
- Ensure that all Internet use should be appropriate to staff professional activity or to student's education.
- Act as good role models in their use of the Internet, computers and mobile devices.
- Plan e-safeguarding programmes as part of our new Computing scheme and within the Digital Literacy strand of the curriculum. Regularly update e-safeguarding programmes to reflect changes in the use of online and digital devices in and out of school.
- Not mention school, pupils or school staff in relation to work on any social media sites.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted using the school email system. Similarly use of personal email addresses for work purposes is not permitted. As part of the 1:1 iPad provision, pupils in Year 5 and Year 6 have access to the same school-based email account via the Microsoft Exchange which goes through a secure socket.

Photos and videos

Digital media such as photos and videos are covered in the e-safeguarding agreement. All parents must sign this agreement to give their consent to photos and videos being published electronically. Non-return of the permission slip will not be assumed as acceptance.

Social Networking

The School has an active Twitter presence where regular updates regarding school events and pupils' achievements are posted. The school's P.T.A. also hosts a "Friends of Nether Alderley" facebook page. Images are used only where permission has been granted to do so. Full names of pupils are never used via social networking sites.

Class Dojo

Class Dojo is used as an effective communication tool between the School and parents. It is operated on an invitation-only basis.

Mobile Phones

- **Staff** are not permitted to use personal mobile phones in school during working hours when in contact with children.
- **Children** are not allowed to use mobile phones in school.

Any other technology

Staff: know that privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head teacher or ICT subject leader;

Children should not bring in their own equipment unless asked to do so by a member of staff.

In addition, the following is to be strictly adhered to:

- Permission slips (via the e-safegaurding agreement) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".

- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy
Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents
Any e-safeguarding incident is to be brought to the immediate attention of the e-Safeguarding Officer, or in his absence the Headteacher. The e-Safeguarding Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues.

E-Safeguarding for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupils' learning via planned and progressive Digital Literacy lessons.

We will establish further training or lessons as necessary in response to any incidents.

The e-Safeguarding Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Handling E-safety incidents and complaints

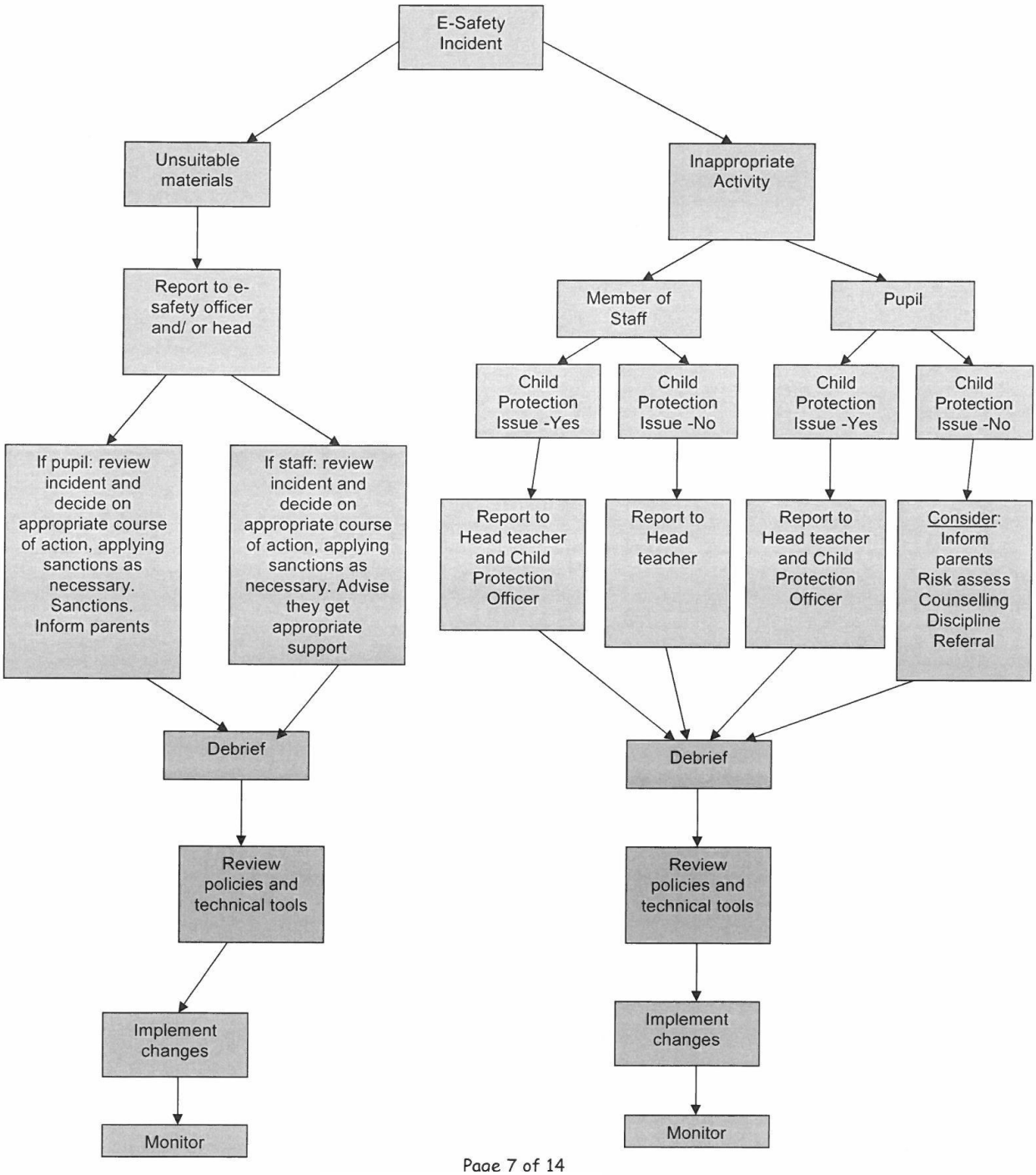
Incidents of Internet misuse will be dealt with by the E-safeguarding Officer. Any incident will follow the referral process below (see Annex 2).

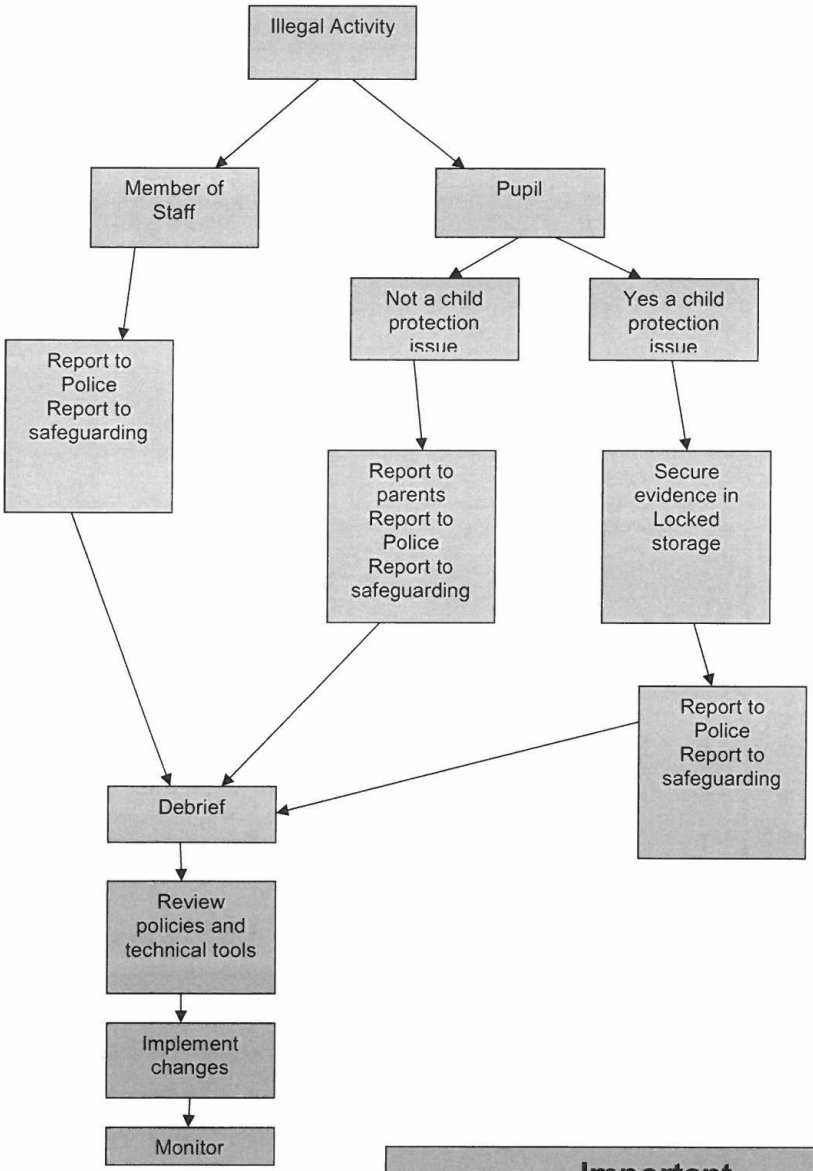
Annex 1

Nether Alderley Primary School e-Safeguarding Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Date reported to Governors			
Signature (Governor)		**Date:**	

Flowchart for referral process for any E-safety incident or illegal activity





Important

Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

Annex 3

Nether Alderley Primary School- E-Safety Agreement – Stay Safe Online

Think SMART when online

We are SMART users.

We keep our personal details SECRET. We never give out our personal details. We never arrange to meet someone we do not know.

We only use the internet when there's a MEMBER of staff or responsible adult present or if we have permission to use it.

We only use our own ALLOCATED login and password.

We will make sure the website we are on is RELIABLE because school can check our files and history on the internet.

We will TELL a member of staff if we see something rude, offensive or inappropriate on the computer.

Child's agreement

Name : _____

- I have read and understand the e-safety rules.
- I will use the computer, internet access and other digital equipment in a responsible way at all times.
- I know that my behaviour and activity will be monitored.
- I understand that if I break the e-safety rules my access to the network may be suspended. If this happens my parents will be informed.

Signed :_____ Date : _____

Parent or Carer's agreement

Consent for web publication of work and images
I agree that my child's work may be published electronically. I also agree that appropriate images and videos that include my child may be published electronically providing that they do not identify my child by name.

Consent to internet access
I have read and understand the e-safety rules. I give permission for my child to access the internet. I understand that school will take all reasonable precautions to ensure that my child is a safe and responsible digital user. I understand that school cannot be held responsible for the content of materials accessed through the internet but I expect that school will take appropriate action in accordance with the e-safety rules. I agree that school is not liable for any damages arising from the use of digital technology. I will support my child by demonstrating safe and responsible use of digital technology.

Signed :_____ Date : _____

Dear Parent/Carer,

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices (such as iPads)
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras

Nether Alderley Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online e-Safeguarding policies and procedures alongside the School's safeguarding measures.

The School takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment.

Full details of the school's E-Safety Policy is available on the school website or on request.

We request that all parents/carers support the schools approach to e-Safety by role modelling safe and positive online behaviour for their child and by discussing online safety with them. Parents/carers can visit the school website for more information about the school's approach to e-safeguarding as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online.

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about e-safeguaring, we request that you read the attached E-Safeguarding Agreement with your child and that you and your child discuss the content and return the signed agreement. Hopefully, you will also find this E-Safeguarding Agreement provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact Mr Brady as the school's E-Safety Officer.

Yours sincerely,

Richard Craven
Headteacher

Annex 4

Nether Alderley Primary School - Staff and Volunteer's E-safety agreement

I appreciate that digital technology includes mobile phones, digital cameras, games consoles and communication methods including email, social networking, instant messaging, twitter and blogs.

I will not disclose any password or security information that allows access to the network.

I will not install any additional hardware or software without permission.

I understand that the police will be involved if my use constitutes a criminal activity and the necessary disciplinary/ allegations processes may be invoked.

I will ensure that personal and confidential information is stored and transmitted securely in accordance with the information sharing requirements of this school.

I will not use my personal equipment for school business without permission from the headteacher.

I will promote e-safety with all children and young people I come into contact with in my role.

I will ensure that any electronic communications I may make with any child or young person, colleague or external professional, are compatible with my professional role. I will ensure that these messages are polite and respectful and cannot be misunderstood or misinterpreted.

I will act as an e-safeguarding role model for all children and young people I come into contact with in my role.

I will report any incidents of concern, including unsuitable personnel activity or content, to the E-safeguarding officer and the Designated Child Protection Officer and the Head Teacher.

I will make sure that any personal use of the system conforms to this e-safety agreement.

I will make sure that any personal social networking sites, email accounts etc are set up securely. I will not allow access to my personal accounts to any child or young person I am working with in a professional role.

Staff and Volunteer agreement

I have read, understand and accept the Nether Alderley Primary School Staff and Volunteer e-safeguarding rules for those who work with children and young people, their parents or carers.

I will promote safe and responsible use of digital technology at all times.

Signed :_____ Date : _____