E-safety and Acceptable Use Policy 2015-2018

Purpose

This policy details Avenue Junior's safeguarding arrangements including rules and guidance pertaining to the use of technology for all school users both within and outside of school. The policy's purpose is:

- to protect and educate pupils and staff and other school technology users in their use of technology so as to ensure all stakeholders are safeguarded,
- to set out the appropriate mechanisms to intervene and support any incident where appropriate,
- to ensure that the school is not exposed to legal risks,
- to ensure that the reputation of the school is not adversely affected by inappropriate use,
- to establish clear guidelines for staff on what they can and cannot do to keep themselves safe and protected against allegations,
- to ensure that the school is able to manage conduct effectively.

Summary

- E Safety risks can be categorised into three areas; contact, content and conduct.
- Compliance with this policy will help to ensure that the benefits of using technology, both online and off-line, can be realised safely, minimising and managing the risks from the 'three Cs'.
- All members of the school community must agree to use technology in a safe and responsible manner.
- Failure to meet the expectations set out in this policy may result in disciplinary action being taken.
- Each member of the school community has a responsibility for their own E Safety and also for that of others.
- A full policy is available on request from the school office.
- This policy is in line with Norfolk County Council incorporating **P319 Internet (including social networking) and email usage in schools and academies – Model policy (Appendix 1)** and complies with the **legal framework surrounding E-safety (Appendix 2)**

Status
Recommended

Who/what was consulted
This policy has been written by Debbie Dismore (Designated Staff and Head Teacher), Mike Hooper (Deputy Headteacher and ICT Leader) and Amanda Norman (TLP Governor). All staff have been consulted.

Relationship to other Policies

- Whole School Policy for Safeguarding, including Child Protection
- Whistleblowing Policy
- Anti Bullying Policy
- Ready to Learn: Positive Behaviour and Discipline Policy
- Mobile Phone Policy
- Curriculum Policy
- Staff Code of Conduct

Arrangements for monitoring and evaluation

- The Governing body will review E-safety arrangements as part of the annual safeguarding review in light of up to date and relevant guidance on E-safety.
- The Deputy Headteacher will monitor the effectiveness of the policy and report to the Headteacher and Well-being and Environment Committee annually where the policy will be reviewed.
- Any incidents of cyber bullying will be recorded on the Bullying Log, which is reported on (protecting identity of all children) 4 times a year at TLP Committee meetings and annually to the Full Governing body.

Contents

1. Introduction

The use of technology, including the internet, emails and social networking sites has grown significantly and has vastly increased opportunities for teaching and learning. However, abuse and misuse of this technology, in terms of inappropriate use, has seen a significant increase in the number of disciplinary cases against staff nationally and increased potential E-safety risks posed to children in school. This policy is written to apply to all employees and volunteers (including governors) in school as well as offering guidance for pupils in their safe and appropriate use of technology. It is designed to form part of the school's overall E-safety framework.

The school expects employees, children and volunteers working in the school to adhere to this policy in line with the school's obligations under equality legislation. The Headteacher must ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless of age, gender, ethnicity, sexual orientation, disability, faith or religion, gender identity, pregnancy or marital status.

Appropriate sections of this policy will identify risks (the 'three Cs') and how they can be managed from the point of view of staff, children and volunteers. Other sections will offer guidance and instruction that is not separated into 'content, contact and conduct'.

2. Internet use

The internet is a valuable resource for teaching and learning and is used regularly in schools. However, it can also present a high level of risk if it is abused or if safe practices are not adopted.

2.1 Internet Conduct

- Staff are instructed not to use school equipment to access the internet for private purposes unless they have permissions from the headteacher.
- Staff should be aware that the network and internet use is closely monitored and individual use may be traced.
- Inappropriate use of these facilities may constitute a criminal or disciplinary offence.
- All school technology users must maintain confidentiality of personal and private information, including username and password information.
- Children must only use the internet at school under the direction of school staff and not for their personal use.
- Staff will supervise children's access to the Internet.
- Staff should not communicate online whilst identifying themselves as a representative of the school, discuss school matters or bring the school into disrepute with any content they should choose to publish.

- Further advice and guidance regarding what is appropriate use of the internet is available in the ICT code of conduct; this can be found within the E-safety pages of Norfolk Schools.ve Alternatively if employees or managers are unsure of what they can and cannot do they can seek advice from the Online Safety Helpline email: helpline@saferinternet.org.uk or call 0844 3814772.

2.2 Internet Content

- School technology users' use of digital materials should not infringe copyright law.
- No school technology user should search for or post inappropriate, illegal or offensive content online.
- No content posted by any member of staff should bring the school into disrepute.
- The school uses the Norfolk County Council filtering system to try to prevent inappropriate or offensive material appearing on school screens.
- Children will be taught to be critically aware of the reliability of sources of information found online
- The school recognises that inappropriate/offensive content may appear on school screens unintentionally; wherever this is the case, the school technology user must report it following school procedures.
    - In the case of children, the procedure is 'don't delete it, switch off the screen, tell an adult'.
    - In the case of adults the procedure is 'don't delete it, switch off the screen, tell the deputy headteacher or headteacher'.
    - The school will then work with ICT Shared Services to block the content.

2.3 Internet Contact

Children should not contact people online unless given the express permission from staff.

Staff should only allow contact between children and other Internet users if contact is assessed to be safe and strictly supervised.

Internet contact between staff and pupils is only permitted via approved school systems, e.g. VLE, school email. All other forms of contact re strictly prohibited.

3. **Email use**

Email provides a fast effective, environmentally friendly and convenient form of communication between all school stakeholders. As such, the issues

surrounding Content, Contact and Conduct are outlined below to avoid allegations of misuse.

3.1 Email Content

- What is written in an email may have to be released under the Data Protection Act or the Freedom of Information Act. Staff must not include information that may cause embarrassment to them or the school, and must maintain professionalism at all times.
- Always double-check that the email has been addressed to the correct recipient(s).
- If the e-mail concerns an individual, do not name them in the 'subject field'.
- If any school user is uncomfortable about the suitability of email content this should be reported immediately to (in the case of a pupil) a teacher or other adult they are working with at the time. In the case of staff, the email should be shown to the headteacher or deputy headteacher as soon as possible. In either case, the email should not be deleted in case it is needed to be investigated further.

3.2 Email Contact

- Employee to pupil email communication must only take place via the school email account (currently nsix) or from within the learning platform (currently Its Learning).
- Staff and children should be wary of opening email from unknown senders
- Both children and staff will be advised to tell the deputy headteacher or the headteacher if the feel they are experiencing inappropriate contact from any school user. The school's Whistle Blowing policy will apply where necessary.

3.3 Email Conduct

- Employees may only use approved e-mail accounts on the school system
- Children and staff should report misuse of email, including abusive communications and cyberbullying, immediately
- Employees must conduct themselves in a professional ad courteous manner in all forms of communication including email.

3.4 Response to possible misuse of email

Sometimes school users may identify misuse of email if they receive communications that they feel uncomfortable with or know to be against professional guidelines. This should be responded to in the following ways:

- In the case of children, 'Don't delete it, switch off the screen, tell an adult.'
- In the case of staff, 'don't delete it, tell the deputy headteacher or headteacher'
- The headteacher/deputy headteacher will investigate the email and act accordingly in line with the school's procedures for responding to E-safety concerns (other policies may then apply, e.g. Safeguarding, Safe Use of Images, Whistle Blowing, Anti-Bullying)

Further advice and guidance regarding safe use of emails is available in the E-Safety toolkit. This can be found by typing 'e-safety' into the search function on Norfolk Schools.

4. **Data protection, freedom of information and copyright**

4.1 Content issues related to Data protection, freedom of information and copyright

Employees should not copy and paste any images or text from or make links to images on other sites on the internet unless the other site specifically says that the images and/or text have been copyright cleared for use in that purpose.

Employees should remain aware of their data protection and freedom of information obligations. Further information can be found on Norfolk Schools in the Freedom of information and data protection sections.

Consideration should be given to what is being posted with regards to:

- is the information being posted in the public domain?
- has permission been granted to publicise it from the person who created it?
- is the person who created it aware that the material is going to be made available on the internet?

4.2 Contact issues related to Data protection, freedom of information and copyright

- Staff should always be aware of data protection issues when asked for information to be shared. There are different levels of information sharing that may be appropriate for various given circumstances; for example, Safeguarding of children may require information to be shared with the police.

- Staff should always check with the headteacher or the deputy headteacher if asked for information about a child to be shared.
- School email (nsix) accounts are not private and so confidential information should only be sent via head@ or deputy@.

4.3 Conduct issues related to Data protection, freedom of information and copyright

- Staff should not share information that may breach their obligations with regard to data protection, freedom of information and copyright.
- Children will be taught about copyright as part of their Computing curriculum lessons.
- Some uses of technology such as VLE, Sumdog and network access may require a username and password to protect personal information and to safeguard users.
- Staff and pupils must keep personal information private including usernames and passwords for network, equipment or website access. Failure to comply with this may result in disciplinary action.
- Staff should not use external storage devices such as memory sticks to store confidential information unless given express permission by the deputy headteacher or headteacher.
- Staff are responsible for maintaining the security of devices such as laptops where confidential information may be stored and are expected to take reasonable precautions to protect this information.
- Staff should be aware that if they are deemed to have treated confidential information with a lack of care that could place data at risk of breach of data protection, freedom of information and copyright laws then they may be open to disciplinary proceedings.

5. Social networking

Social media is the term commonly used for websites which allow people to interact with each other in some way (social networking) – by sharing information, opinions, knowledge and interests. Social media is part of many people's day to day lives. The following information has been put together for the benefit of employees to help them understand what may be deemed appropriate or inappropriate both inside and outside of work.

Social media is another form of communication and is not necessarily private. Employees should consider if it would not be said to a current or future colleague or parent, pupil or manager then it should not be published on a social networking site, whether this is a school managed site or a personal one.

- Online conduct should be as exemplary as offline conduct. Employees and volunteers must have regard to the fact that anything that is said on the internet could at some point be made public.
- The school recognises that social networking sites, websites and blogs provide a useful tool for communication and learning and are accessed widely. However the safeguarding of pupils and employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:
- Safeguarding of pupils and employees is the responsibility of all employees and this should also be taken into consideration when using personal social networking sites inside and outside of the school. Employees should not link their own personal social networking sites to anything related to the school.
- Employees are advised not to communicate with pupils or accept pupils as friends on social network sites using their personal systems and equipment. Where a member of staff is related to a pupil the school should be made aware, if they are not already, and consideration given to whether any safeguards need to be put in place. Employees should also consider carefully the implications of befriending parents or carers as contacts on social networking sites. No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18.
- Any communication with pupils should take place within clear and explicit boundaries
- If employees use personal social networking sites they should not publish specific and detailed public thoughts or post anything that could bring the school into disrepute.
- Employees must not place inappropriate photographs on any social network space and must ensure that background detail (e.g. house number, street name, school) cannot identify personal/employment details about them.
- Official blogs, sites or wikis must be password protected and overseen and sanctioned by the school/academy.
- Contact should only be made with pupils for professional reasons via professional spaces set up and run by the school. If professional spaces are set up, steps should be taken to ensure the users of the space are not put at risk e.g. privacy settings, data protection and data security. Permission should be sought from the Headteacher and the parents/guardians of pupils to communicate in this way.
- Employees are not permitted to run social network spaces for pupil use on a personal basis. If social networking is used for supporting pupils with work, professional spaces should be created by employees and pupils as

in paragraph above. One example of this would be Sumdog where the features are appropriate to the age of the pupils and of a nature that safeguards them.

- Employees are advised not to use or access the social networking sites of pupils, without due reason e.g. safeguarding purposes.
- If an employee feels they are a victim of cyberbullying they should report it via the appropriate channels, please see below.
- The school has a VLE that does have some features of social networking in so much that users can communicate with other pupils and staff and access resources posted online. The guidance regarding social networks applies in the same way to the school VLE as it does to other forms of social networking.

6. Photographic use in school

Although there is a separate policy entitled 'Safe Use of Images', this section will offer guidance to staff in order to safeguard both pupils and staff.

6.1 Images of Children

- No images of children will be stored on teachers' laptops.
- No images of children will be taken home without express permission of the headteacher or other SMT member (this may be appropriate for assessment records, display work etc.).
- Images should only be captured using school equipment.

6.2 Use of mobile/personal devices

- The use of mobile personal devices by staff is not permitted for taking photos of children in any circumstances.
- However, where parents or other parties have a legitimate personal reason for the use of mobile technologies for image capture, the guidance in the Safe Use of Images Policy will apply.
- Mobile devices may be used freely by staff during break times but should not be used during lessons unless there is a valid and legitimate educational reason, such as playing music to the class as part of a curriculum lesson.
- Children are not permitted to bring mobile phones to school; parents have been informed of this by letter (appendix 3) and a policy statement (appendix 4) has been issued by the headteacher and governing body.

6.3 Video Conferencing

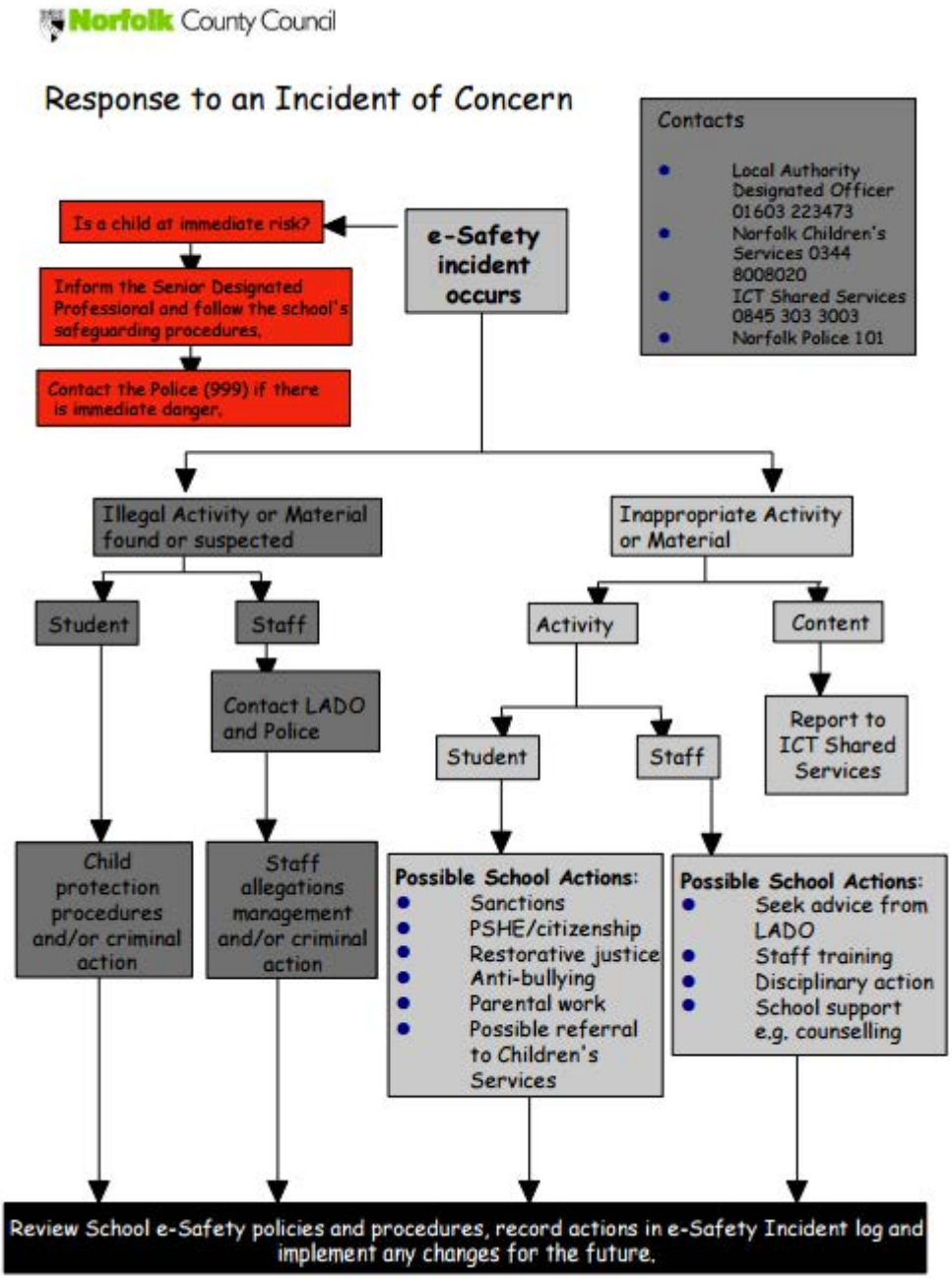
The school has a facility to Skype video chat. There is one school account for which the username and password is held by staff and will only be used under

strict supervision of staff to ensure that any Skype communication is in line with the rest of the E-safety policy.

7. How the school will respond to E-safety concerns

- Complaints of Internet misuse will be dealt with by the E Safety designated teacher.
- All matters of cyber bullying are referred directly to the Head teacher.
- The network manager will monitor use and the children will be responsible for reporting any instances of cyber bullying.
- Parents are made aware of the school's policy of access to social networking sites
- Where a disclosure of bullying is made, the school will investigate and protect, even where the bullying originates outside the school.
- Once disclosure is made, investigation will have to involve the families. This will be dealt with under the school's Anti Bullying Policy. All cyber bullying incidents are referred directly to the Head teacher.
- If parent/carers refuse to engage and bullying continues, it can be referred to the police as harassment
- This guidance will also apply to text and mobile phone cyber bullying.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints against the Headteacher must be referred to the Chair of Governors. (See Whistleblowing Policy). Complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures (see Whole School Safeguarding, including Child Protection, Policy.)
- Any misuse could result in removal from the network and possibly further disciplinary action. This could, if appropriate, include involving external agencies, such as the police.

The following diagram details the procedure of response in line with Norfolk County Council recommendations:



8. Effective communication of this policy

8.1 To staff

- Staff will be required to sign to say they have read this policy
- A summary of the policy will be presented as 'Staff, Governor, Visitor and other Adults Working in School Acceptable Use Agreement/ICT Code of Conduct' (Appendix 5) to be signed by all staff.

- Training for staff on E-safety will be offered to all staff and will form part of Safeguarding training

8.2 To Pupils

- Pupils will be required to sign a 'Pupil Technology Agreement' (Appendix 6) that will summarise the relevant parts of this policy before being able to use technology in school.
- Pupils will regularly participate in lessons about E-safety as part of the curriculum
- The school will participate in the Safer Internet day annually to raise the profile of E-safety in school

8.3 To Parents

- Parents will be required to sign the 'Parent/Carer Technology Agreement' (appendix 7) that will summarise the relevant parts of this policy before their child is able to use technology in school.
- Parents will be able to view a copy of this policy on the school website.
- A copy of this policy will be available from the school office.
- Parents will be given curriculum overviews detailing E-safety lesson content

8.4 To Governors

- This policy will need to be approved by governors.
- The impact of the policy will be reported to the governors by the deputy headteacher
- Instances of cyberbullying will be reported to the governing body
- Governors will be invited to any E-safety related events in school including Internet Safety day

If employees or managers need to seek advice about inappropriate use they can contact the Online Safety Helpline (email: helpline@saferinternet.org.uk or call 0844 3814772). However, employees and managers should not bypass the school's safeguarding procedures.

Appendix 1

P319 Internet (including social networking) and email usage in schools and academies – Model policy

Contents

1. Introduction

The use of the internet, emails and social networking sites has grown significantly and has vastly increased opportunities for teaching and learning. However, abuse of this technology, in terms of inappropriate use, has seen a significant increase in the number of disciplinary cases. This model policy is written to apply to all employees and volunteers (including governors) in the school/academy. It is designed to form part of the school/academy's overall e-safety framework. The purpose of this policy is to ensure that:

- pupils and employees are safeguarded
- the school/academy is not exposed to legal risks
- the reputation of the school/academy is not adversely affected by inappropriate use
- school/academy employees have clear guidelines on what they can and cannot do to keep themselves safe and protected against allegations
- Headteachers / Principals are able to manage conduct effectively

Note: To aid the school/academy in ensuring their e-safety framework is robust and compliant documents can be found on the Norfolk Schools website. Type 'e-safety' into the search.

Non LA maintained schools and academies can choose to adapt and adopt this policy, following appropriate consultation with staff.

Equal Opportunities and Scope

The school/academy expects employees and volunteers working in the school/academy to

adhere to this policy in line with the school's/academy's obligations under equality legislation. The Headteacher/Principal must ensure that all reasonable adjustments or supportive measures are considered to allow equality of access and opportunity regardless of age, gender, ethnicity, sexual orientation, disability, faith or religion, gender identity, pregnancy or marital status.
This policy should be read in conjunction with, and have due regard, to:

- The NCC E- Safety policy
- The NCC E-Safety toolkit }
- The NCC ICT code of conduct for staff, governors and visitors
- The School Teachers Pay and Conditions Document (professional duties and national standards (weblink can be found on Schools' PeopleNet in the 'Pay' section.
- Employee discipline guidelines on conduct for employees (G303e) on Schools' PeopleNet
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings (weblink can be found on Schools' PeopleNet in the 'Standards of conduct and behaviour' section).

2. Internet use

The internet is a valuable resource for teaching and learning and is used regularly in schools and academies. However, it can also present a high level of risk if it is abused or if safe practices are not adopted.
Schools/academies should advise employees not to use school/academy equipment to access the internet for private purposes unless they have permission from the Headteacher/Principal. Employees should be made aware that the network and inappropriate use of the internet is closely monitored and individual usage can be traced.Inappropriate use of these facilities may constitute a criminal or disciplinary offence.

Further advice and guidance regarding what is appropriate use of the internet is available in the ICT code of conduct, this can be found within the e-safety pages of Norfolk Schools. Alternatively if employees or managers are unsure of what they can and cannot do they can seek advice from the Online Safety Helpline email: helpline@saferinternet.org.uk or call 0844 3814772.

3. Email use

- What is written in an email may have to be released under the Data Protection Act or the Freedom of Information Act. Do not include information that may cause embarrassment to you or the school/academy, maintain professionalism at all times.
- Always double-check that the email has been addressed to the correct recipient(s).
- If the e-mail concerns an individual, do not name them in the 'subject field'.
- Employee to pupil email communication must only take place via a school/academy email account or from within the learning platform.
- Employees may only use approved e-mail accounts on the school system

Further advice and guidance regarding safe use of emails is available in the E-Safety toolkit. This can be found by typing 'e-safety' into the search function on Norfolk Schools.

4. Data protection, freedom of information and copyright

Employees should remain aware of their data protection and freedom of information obligations. Further information can be found on Norfolk Schools in the Freedom of

information and data protection sections.

Employees should not copy and paste any images or text from or make links to images on other sites on the internet unless the other site specifically says that the images and/or text have been copyright cleared for use in that purpose.

Consideration should be given to what is being posted with regards to:

- is the information being posted in the public domain?
- has permission been granted to publicise it from the person who created it?
- is the person who created it aware that the material is going to be made available on the internet?

5. Social networking

Social media is the term commonly used for websites which allow people to interact with each other in some way (social networking) – by sharing information, opinions, knowledge and interests. Social media is part of many people's day to day lives. The following information has been put together for the benefit of employees to help them understand what may be deemed appropriate or inappropriate both inside and outside of work.

Social media is another form of communication and is not necessarily private. Employees should consider if it would not be said to a current or future colleague or parent, pupil or manager then it should not be published on a social networking site, whether this is a school/academy managed site or a personal one.

Online conduct should be as exemplary as offline conduct. Employees and volunteers must have regard to the fact that anything that is said on the internet could at some point be made public.

The school/academy recognises that social networking sites, websites and blogs provide a useful tool for communication and learning and are accessed widely. However the safeguarding of pupils and employees is of paramount importance, adults should lead by example and set standards of behaviour. Therefore:

5.1. Safeguarding of pupils and employees is the responsibility of all employees and this should also be taken into consideration when using personal social networking sites inside and outside of the school/academy. Employees should not link their own personal social networking sites to anything related to the school/academy.

5.2. Employees are advised not to communicate with pupils or accept pupils as friends on social network sites using their personal systems and equipment. Where a member of staff is related to a pupil the school/academy should be made aware, if they are not already, and consideration given to whether any safeguards need to be put in place. Employees should also consider carefully the implications of befriending parents, carers or ex-pupils as contacts on social networking sites.

5.3. Any communication with pupils should take place within clear and explicit boundaries

5.4. If employees use personal social networking sites they should not publish specific and detailed public thoughts or post anything that could bring the school/academy into

disrepute.

5.5. Employees must not place inappropriate photographs on any social network space and must ensure that background detail (e.g. house number, street name, school/academy) cannot identify personal/employment details about them.

5.6. Official blogs, sites or wikis must be password protected and overseen and sanctioned by the school/academy.

5.7. Contact should only be made with pupils for professional reasons via professional spaces set up and run by the school/academy. If professional spaces are set up steps should be taken to ensure the users of the space are not put at risk e.g. privacy settings, data protection and data security. Permission should be sought from the Headteacher/Principal and the parents/guardians of pupils to communicate in this way.

5.8. Employees are advised not to run social network spaces for pupil use on a personal basis. If social networking is used for supporting pupils with coursework, professional spaces should be created by employees and pupils as in paragraph 5.7 above.

5.9. Employees are advised not to use or access the social networking sites of pupils, without due reason e.g. safeguarding purposes. However, this may not be possible to achieve if the situation in 5.2 applies.

5.10. If an employee feels they are a victim of cyberbullying they should report it via the appropriate channels, please see below.

If employees or managers need to seek advice about inappropriate use they can contact the Online Safety Helpline (email: helpline@saferinternet.org.uk or call 0844 3814772). However, employees and managers should not bypass the school/academy's safeguarding procedures.

6. The consequences of improper/unacceptable use of social media, the internet and email

6.1. The Headteacher/Principal can exercise their right to monitor the use of the school/academy's information systems and internet access. This includes the right to intercept email and the right to delete inappropriate materials where they believe unauthorised use of the school/academy's information system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised text, imagery or sound.

6.2. Employees must be aware that improper or unacceptable use of the internet or email systems could result in legal proceedings and the use of the school/academy's Disciplinary Procedure. Sanctions will depend upon the gravity of misuse and could result in summary dismissal in some cases.

7. Monitoring

This policy relies on employees acting responsibly and in accordance with the outlined restrictions. Where employees have concerns that a colleague is acting in breach of the outlined restrictions, they are encouraged to raise this with the Headteacher/Principal or Chair of Governors if the concerns relate to the Headteacher/Principal.

If the concern involves possible inappropriate interaction between a colleague and a pupil, referral may be made to the designated senior professional in the school/academy.

8. Further information

- Child exploitation and Online Protection (CEOP) website – internet safety
- HR Direct: HRDirect@norfolk.gov.uk / 01603 222212

Appendix 2: The Legal Framework surrounding E-safety

This section is designed to inform users of legal issues relevant to the use of electronic communications. The law is developing rapidly

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006, sections 90 and 91, provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. Section 94 also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with E-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also

covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to Wellbeing and Environment Committee know that his course of conduct will cause the other so to fear on each of those occasions.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from abuse based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003

A new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and then intentionally meet them or travel with intent to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence

for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, etc.).

Any sexual intercourse with a child under the age of 13 commits the offence of rape. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document, which is available from the Home Office website (www.homeoffice.gov.uk/documents/children-safer-fr-sex-crime?view=Binary).

More information about the 2003 Act can be found at www.teachernet.gov.uk

Appendix 3

NORFOLK COUNTY COUNCIL

AVENUE JUNIOR SCHOOL

AVENUE ROAD, NORWICH, NORFOLK, NR2 3HP

Head Teacher: Mrs. Debbie Dismore B.Ed. (Hons.)

Telephone: Norwich (01603) 441034 Fax: (01603) 441035

Email: office@avenuejunior.norfolk.sch.uk

www.avenuejuniorschool.org

6th January 2015

Dear Parent/Carers,

Re: Concern about misuse of mobile technology in school

I am writing to remind you of school policy regarding mobile phones and electronic devices. **Mobile phones and other electronic devices which can access the internet, including Ipods, tablets and smart watches, are not allowed in school.**

There are many reasons for this policy:

1. To ensure the privacy and safety of all children
2. To limit the risk of damage to the emotional well-being of children, including access to potentially unsuitable materials
3. To avoid peer pressure and competitiveness regarding the make and model
4. To avoid disruption to pupils learning
5. To avoid theft, loss and damage of valuable items
6. The internet is accessed very safely at school and so we cannot allow other internet- ready devices to be brought into school that do not have the same filtering systems and which could possibly be accessed by children without supervision.

We have witnessed on many occasions this year an increased risk of bullying on electronic devices, as well as the potential misuse of them, including the issues surrounding the safe use of the camera facilities. Children's safeguarding must always be paramount and we cannot allow technology into school where images could be captured and then downloaded at home. Adults in school are also required to adhere to clear guidelines about the use of technology (the Mobile Phone Statement and E Safety and Acceptable Use Policy 2012 – 2015 can be found on the school website.).

We acknowledge that some parents feel that their children may be safer with a mobile phone when walking to and from school. However, there are reports which highlight the fact that of all mobile phones that are stolen, a large proportion of these are taken from children and young people.

I hope that this helps you to understand the reasons for this ban on mobile phones and electronic devices and that you will help us to ensure the safety and well-being of your child and others by making sure that they leave such technology at home.

Social Media

Social media and technology will play an ever increasing role in your children's lives; we have a duty to ensure they take full advantage of this but use it safely and appropriately for their age. We have been asked by the Governing Body and a number of parents to produce some guidelines offering support to help you ensure your child remains safe at home whilst using technology. These guidelines

are in line with the advice given by social media sites. You will find these with this letter and I hope that they will be useful to you.

Yours faithfully,

Mrs Dismore, Headteacher

Computers and the Internet – A Parents' Guide

Your children are growing up in an exciting and fast paced modern world and it can sometimes be tough just to try to keep up with them! The following guidance is purely based on information gathered from various reputable resources and is there just to guide you should you want the support rather than to tell you how to parent your children!

Behaviour is behaviour whether it happens in the 'real' offline world or the 'virtual' online world and as parents, we need to think about how to set boundaries to help guide our children to behave well and reduce the risk of harm to them or others in both the offline and online worlds.

Although there is no official guidance about healthy amounts of screen time, the Central London Community Healthcare Trust (CLCH NHS) has produced a leaflet stating that screen time should be 'strictly limited' for children under 2 and restricted to 2 hours maximum each day for older children.

Microsoft has issued guidance for parents that states that children should have an adult with them to supervise their internet use until they are at least 10 years old. It's important to remember that there are a large number of wide ranging devices that can access the internet from iPods and iPads to phones, laptops and pcs – even TVs and games consoles! We need to make sure that, as parents, we know when and where our children are online and what they are doing and viewing.

Childnet International writes, 'children and young people…need support and guidance when it comes to managing their lives online and using the internet positively and safely.' They have some fantastic information on their website and advise open communication between parents and children about the internet – helpfully, they include some useful conversation starters to help to get going!

The internet is a wonderful and exciting resource that can have a tremendous impact on all kinds of aspects of children's lives and with support of parents, it is hoped that our pupils will behave safely and with care to others in the online world.

CLCH screen time leaflet -
http://www.clch.nhs.uk/media/128453/screen_time__early_development.pdf

Great advice on this official site including practical technical support to help parents to keep children safe online - https://www.thinkuknow.co.uk/parents/Primary/

Age related Internet use advice from Microsoft - http://www.microsoft.com/en-gb/security/family-safety/childsafety-age.aspx

Childnet International advice for parents - http://www.childnet.com/parents-and-carers

Appendix 4

Mobile Phones and Electronic Devices at Avenue Junior School

Policy Statement

The Headteacher and governors have agreed that children are not allowed to bring mobile phones in to School. This also applies to all other electronic devices, such as tablets and iPods, which can access the internet. While we acknowledge that mobile phones are a routine part of everyday life for many children (but by no means all at this age), the School's policy is that they should not be brought to School for the following reasons:

- Mobile phones can disrupt learning, particularly if they are kept in pockets or desks. The alternative, i.e. keeping them in children's bags in the cloakrooms, may present opportunities for theft.
- Issues surrounding peer pressure and competitiveness have increased as a result of children bringing in mobile phones. There is also a greater risk of cyber bullying and potential for misuse, and increasingly so with phones that have internet access.
- To ensure the privacy and safety of all children.
- To limit the risk of damage to the emotional well-being of children, including access to potentially unsuitable materials.
- The School cannot accept responsibility for phones should be they be lost, damaged or stolen. There is no capacity within the school office to book every phone brought to school in and out each day.
- The School does not believe that having a mobile phone keeps a child safe.

Should a child be found to have a mobile phone or other electronic device in school, the item will be retained by staff and parents will be asked to collect the item at the end of the school day.

Agreed at FGB 27/4/2015

Appendix 5:

Staff, Governor, Visitor and other Adults Working in School Acceptable Use Agreement/ICT Code of Conduct

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is an offence to use a school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my username
- I will ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any school business
- I will ensure that all data is kept secure and is used appropriately and as authorised by the Head teacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.
- At school, I will not install any hardware or software without the permission of Avenue Junior School.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images will only be taken, stored and used for purposes in line with school policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the school network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Head teacher.

- I understand that my permitted use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Senior Designated Professional or Head teacher.
- If I have any other E-safety concerns regarding content, contact or conduct then the relevant reporting procedures should apply.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full name:……(printed)

Job title:…….

Signature:……Date:……

Appendix 6: Pupil Technology Agreement

Using technology is really valuable as it helps us to learn. To make sure that everyone can enjoy learning with technology and stay safe. I agree that:

- I will keep my personal usernames and passwords completely private (including my
- VLE details).
- I will try to make sure that I can trust the information I see online by checking it on more than one site.
- If I see something I feel uncomfortable about or I think is unacceptable I will switch off the screen and tell an adult.
- My teachers can check what I've been doing on technological devices.
- At school, I will only use the email account given to me by my teachers.
- When I share anything online, including on VLE, I will always do so with respect for other people.
- I will never deliberately hurt someone else's feelings online.
- If somebody from another school shares something with me on VLE, I will show it to my teacher.
- If somebody says something unkind about me or anyone else online, I will tell an adult and my school will help to sort out the problem, even if it happened outside of school.
- If I become aware of any kind of cyberbullying, I will tell an adult straight away.
- I will not use social networking sites (like Facebook and MSN) to contact my teachers
- or anyone else although I can use VLE and my email for this.
- I will not post any pictures of myself online without the permission of my teachers.
- I will never meet strangers who I have spoken to online.
- I will never tell anyone personal details about myself on the Internet.
- I will not bring a mobile device, such as mobile phone or iPod, to school.
- I will treat our school equipment carefully.
- I will always log off when my computer session has finished.

☐ Tick this box if you have permission to use an authorised Personal Device for learning (e.g. laptop)

- No personal devices can be linked to the school network.
- The school cannot accept any liability for any damage to or loss of personal devices; and these should be covered by family insurance.
- If this device is used inappropriately outside of the lesson, the school cannot be held responsible. If any misuse (as per School Policy) is discovered this device will be confiscated until the end of the School Day.

I keep to this agreement so that everyone can be happy and safe to enjoy learning

online.

Name……..

Signed…….

Appendix 7: Parent/Carer Technology Agreement'

Parent/Carer name: ……

Pupil name: ……

Pupil's Class: ……

- As the parent or legal guardian of the above pupil, I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school email and other ICT facilities at school.
- I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible Information Communication Technology (ICT) use, outlined in the E Safety and Acceptable Use Policy. I also understand that my son/daughter may be informed if the rules have to be changed during the year. I know that the latest copy of the E Safety and Acceptable Use Policy is available on the website, www.avenuejuniorschool.org; or from the school office.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching E-safety skills to pupils.
- I will not allow my child to bring in a mobile device, such as mobile phone or iPod, to school without permission. If permission is granted, the device will when be stored in the office during the school day. The school cannot accept any responsibility for any loss/damage that may occur.
- I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour.
- I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.
- If I become aware of an E-safety concern about any child, I will report it to the appropriate authorities including the school
- If my child receives communication that raises E-safety concerns, I know I should not delete it and that I can notify the school.

☐ Tick this box if you have permission to use an authorised Personal Device for learning (e.g. laptop)

- No personal devices can be linked to the school network.
- The school cannot accept any liability for any damage to or loss of personal devices; and these should be covered by family insurance.
- If this device is used inappropriately outside of the lesson, the school cannot be held responsible. If any misuse (as per School Policy) is discovered this device will be confiscated until the end of the School Day.

Parent's signature:…… Date:……