AVONDALE PREPARATORY SCHOOL

E-Safety Policy

Contents

1. Policy Statement

1.1 E-Safety encompasses not only Internet technologies but also electronic communications such as mobile devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks, and responsibilities of using information technology, providing safeguards and awareness for users to enable them to control their online experiences.

1.2 Most Internet use in school is safe, purposeful, and beneficial to learners. However, there is always an element of risk. Even an innocent search can occasionally lead to inappropriate content. Fast website access means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content.

1.3 Curriculum Internet use provides significant educational benefits, including access to information worldwide and the ability to communicate and publish widely. Internet use in school should be planned, task-oriented, and educational within a regulated and managed environment.

1.4 All staff must read and sign the 'Acceptable Use' documentation. Whenever the policy undergoes significant changes, a new agreement will be required.

1.5 This policy applies to all members of our school community.

1.6 Avondale Preparatory School is committed to ensuring that this E-Safety policy is applied fairly, in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.

1.7 This policy is implemented through adherence to the procedures outlined in this document.

1.8 This document is available on the school website and upon request from the school office. It should be read in conjunction with the following policies:

- Acceptable Use Policy
- Cyber Bullying Policy
- Anti-Bullying Policy
- PSHE Curriculum

1.9 Staff should feel confident in using the Internet for teaching. The E-Safety Policy will be effective only if all staff subscribe to its values and methods. Training and discussions should be provided for staff to develop appropriate teaching strategies.

1.10 Internet use is widespread, and all staff, including administrative staff and volunteers, should be included in awareness training. New staff inductions should include guidelines on appropriate Internet use.

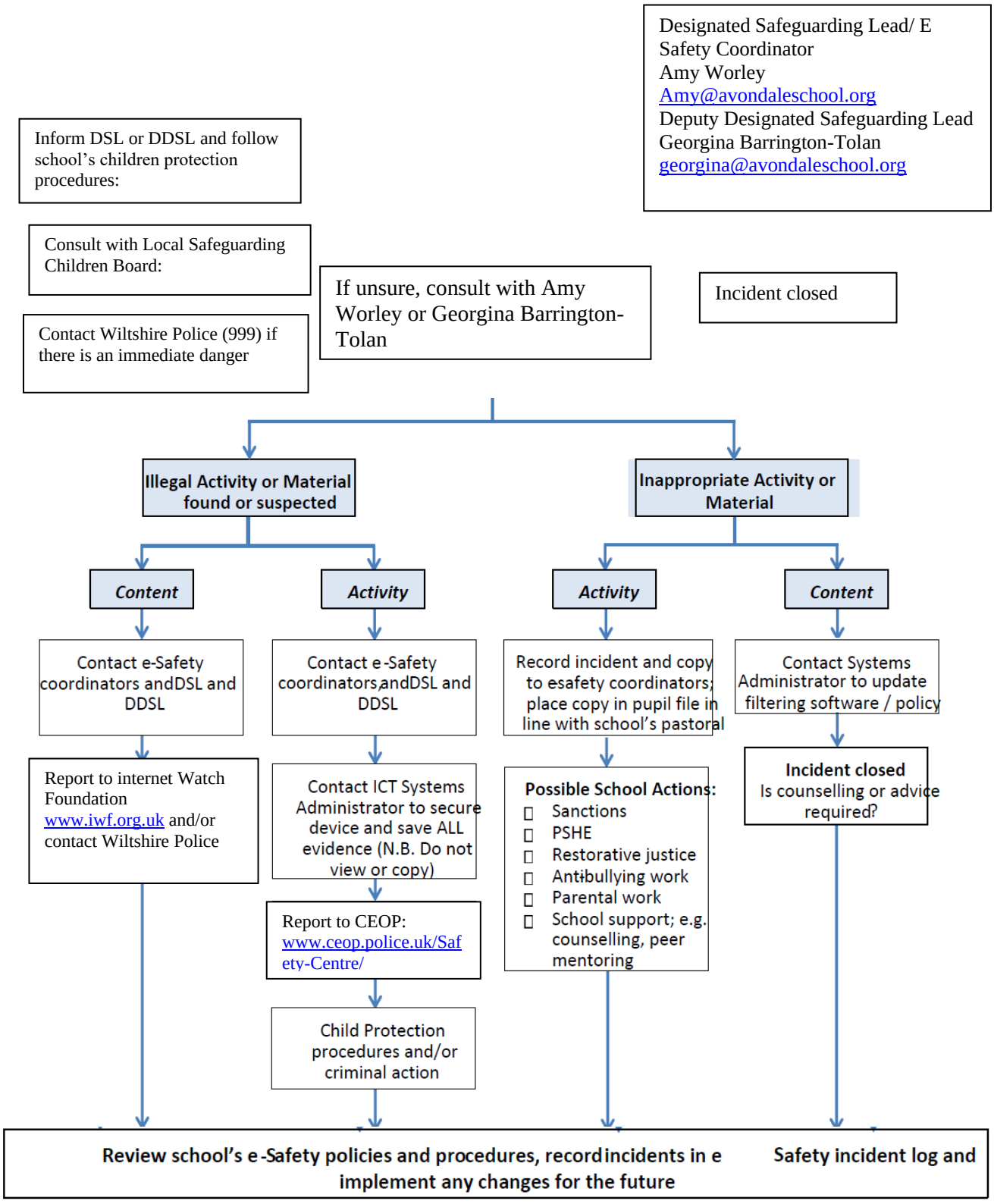
1.11 The school allocates Internet access for staff and pupils based on educational need. Since the quantity and breadth of information on the Internet continues to grow, it is not possible to guard against every undesirable situation.

1.12 **Disclaimer:**
Avondale Preparatory School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

1.13 The school will maintain a record of all staff and pupils granted Internet access. All staff, pupils, and parents must read and sign the Acceptable Use documentation before using any school ICT resource.

1.14 At **Key Stage 1**, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.

2. E- Safety Incident Process



3 E-Safety Complaints

3.1 Prompt action will be required if a complaint is made regarding material accessed on the net, either incidentally or otherwise, or in the event of an accusation of cyber-bullying, etc. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

3.2 A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school's DSL or DDSLs.

3.3 The following overall principles apply:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Procedures will be followed according to the Child Protection Policy.
- Sanctions within the school discipline policy include: – interview/counselling by headteacher; – informing parents or carers; – removal of Internet or computer access for a period.

4 Email

4.1 E-mail is an essential means of communication for both staff, pupils and parents. Directed e-mail use can nurture significant educational benefits.

4.2 In the school context, e-mail should not be considered private and Avondale preparatory reserves the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of staff and pupils and the preservation of human rights, both of which are covered by recent legislation.

4.3 It should be noted that, e-mail that has been provided by the school is to be used only for school business and that personal data is not to be stored anywhere on the Share Point.

4.4 The following general points should be noted by staff:

- Pupils may only use approved e-mail accounts on the school system and access to external personal email accounts is blocked during the working day.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils should not E-mail external organisations unless authorised before sending.
- The forwarding of chain letters is not permitted.

5 Publishing of Pupil Images

5.1 Photographs that include pupils add a liveliness and interest to a Website or blog that is difficult to achieve in any other way. Nevertheless, the security of staff and pupils must come first. Sadly, although common in newspapers, the publishing of pupils' full names (including surname) with their photographs is not acceptable. Web images could be misused and individual pupils identified unless broad descriptions are used.

5.2 Photographs of a pupil should not be published without the parent's or carer's written permission. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

6 Social Networking Access

6.1 Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments. For use by responsible adults, social networking sites provide easy to use, free facilities; although they often feature advertising intrudes and may be dubious in content.

6.2 Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published:

- Examples include: blogs, wikis, Facebook, Twitter, Snapchat, Instagram, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger, P2P sites and many others.
- Avondale will block/filter access to social networking sites during normal working hours.
- Pupils are to be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for students on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students should be advised not to publish specific and detailed private thoughts.
- The school should be aware that bullying can take place through social networking particularly when a space has been setup without a password and others are invited to see the bully's comments.

6.3 This advice is communicated to pupils through presentations, Safer Internet Day events, the PSHE programme and through the tutorial programme.

7 Data Protection

7.1 As part of its everyday activities, Avondale will use or "process" personal data. Details of the type of data we collect and the way it is used can be found in our Privacy Notice www.wiltshire.gov.uk/article/10020/Introduction

7.2 The Data Protection Officer for Avondale Preparatory School is Georgina Barrington-Tolan. She is responsible for ensuring that the school complies with Data Protection Law. She can be contacted on georgina@avondaleschool.org

7.3 Everyone who uses or accesses school systems has a responsibility to protect the data we hold. Pupils should not give access to school systems (by sharing their user id or password) and should not transfer data (including photographs) outside of the school network with specific permission to do so.

8.Sites for reference and e-Safety Guidance

- ***Child Exploitation & Online Protection Centre*** http://www.ceop.gov.uk/contact_us.html
- ***Virtual Global Taskforce – Report Abuse*** http://www.virtualglobaltaskforce.com/
- ***Think U Know website*** http://www.thinkuknow.co.uk/
- ***Internet Watch Foundation*** http://www.iwf.org.uk/
- ***Internet Safety Zone*** http://www.internetsafetyzone.co.uk
- ***Kidsmart*** http://www.kidsmart.org.uk/
- ***NSPCC*** http://www.nspcc.org.uk/
- ***Childline*** http://www.childline.org.uk/
- ***Stop Text Bully*** http://www.stoptextbully.com
- ***NCH – The Children's Charity*** http://www.nch.org.uk/stories/index.php?i=324

9 Relevant Legislation

9.1 The Computer Misuse Act 1990 - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data.
The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

9.2 Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

9.3 Communications Act 2003 - There are 2 separate offences under this act of relevance:

- sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
- sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

10 Acceptable Use Policies

All students and staff are required to subscribe to the school's Acceptable Use Policies. These policies share core themes outlining the need for responsible and safe use of school PCs and internet access. These AUPs are differentiated for different year groups to enable necessary e-safety education to occur at all stages.

11.3 Acceptable use policy for staff

1 Policy statement

1.1 Avondale provide computers for staff use; access to the internet provides vast, diverse, and unique digital resources. Our goal in providing this access is to promote educational excellence by facilitating resource sharing, innovation and communication.
1.2 Digital resources in our context refer to school Information and Communications Technology systems and equipment (such as desktop computers, laptops, tablets and other mobile devices, printers, scanners, photocopiers and other peripherals), but also to programs, applications and services available on the network or on the Internet. Therefore, we expect that this agreement is adhered to both in School and when our digital resources are accessed remotely.
1.3 Teachers, support staff, students and members of the wider school community at Avondale are encouraged to use our digital resources as a way to create and share content and resources, as well as a means to connect with others and network within and outside the school community, always with the overarching aim of supporting and enhancing teaching and learning.
1.4 Tablets and computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and to help to ensure they remain available to all.

2 Ethos

2.1 The School's rules are summed up in the words: Ready, Respectful and Responsible. The School therefore expects its digital resources to be used in this spirit.

2.2 The School expects the members of the School Community to show respect and consideration for self and others and to behave kindly and appropriately, and in such a way that would not disrupt the use of our digital resources.

2.3 The School will not tolerate any form of bullying or deliberate misuse.

2.4 The School expects the members of the school community to use good judgement and behave in such a way that will reflect well on them and the School.

3 Internet

3.1 Users access the Internet only for school activities. However, the filtering system down by SLT allows for personal use after 4pm. Privacy is not guaranteed and restrictions to non-business sites may be applied. Any personal data created or accessed by employees through e-mail, the internet or through any computer programme may be viewed or accessed by the school without the employee's permission.

3.2 Staff should not issue the school web address to any site that is filtered and therefore is intentionally inaccessible from the school network (e.g. some social networking sites). Staff should also not issue their work e-mail addresses to any companies that may generate excessive junk mail.

3.3 Users shall not visit, download from, upload to or otherwise access websites or other electronic media displaying or promoting pornography, child sex abuse images, racial or religious hate, illegal activity or other potentially offensive material.

3.4 Deliberate access to websites or other electronic media containing child sex abuse images, material in contravention of the Obscene Publications Act 1959 and 1964 or material inciting racial hatred will be reported to the police.

3.5 Users shall not use Avondale resources for running a private business.

3.6 Users shall not visit or post to websites or other electronic media that may be defamatory to the school or bring the school into disrepute. Defamation of the school would be seen as a breach of an employee's contract of employment.

3.7 Users shall not visit, upload or download from websites or other electronic media which may cause the user or school to contravene the Copyright, Designs and Patent Act 1988. Refer to section d) below on Copyright.

3.8 Users shall not visit, upload or download from websites or other electronic media which may cause the user or school to contravene the Data Protection Act 1998.

3.9 Users shall not attempt to interfere with the normal operation of the school's ICT resources by propagating or attempting to propagate viruses, spyware, malware or other malicious code.

3.10 Users must obtain prior approval at Senior Leadership level to set-up internet sites on school computer facilities, publish pages on external internet sites containing information relating to the school, enter into agreements on behalf of themselves or the school via a network or electronic system, transmit unsolicited commercial or advertising material to other users of a network or to other organisations and use school computing facilities for external gain.

3.12 Users will inform the Designated Safeguarding Lead if they accidentally encounter inappropriate material whilst using the School's digital resources.

3.13 Avondale will routinely monitor and audit the use of the internet to ensure compliance.

3.12 On evidence provided, a user may be disciplined by the school. At the same time, if a user behaves in an unlawful way, the user's behaviour may be reported to the police.

4 Email

4.1 Work or activity conducted through email must be directly related to your school work.

4.2 Staff must not give their password or login name to anyone, except to a member of the IT support or Headteacher.

4.3 Users shall not download, use or upload or send by email any material which in doing so infringes copyright and they must not view, upload or download or send by email any material which is likely to be unsuitable for children or schools. This applies to material of a violent, dangerous, racist or inappropriate sexual content. If you are unsure about this, or any materials, you must ask your line manager.

4.4 Be polite and appreciate that other users might have different views from your own. The use of strong language, abusive language (swearing) or aggressive behaviour is not allowed. You should not write anything on a website or send by email anything which could be offensive. If you receive an email containing any of the above always report such messages to a member of the IT support team.

4.5 Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

4.6 Avondale may monitor without notice external and internal email and has the right, if it wishes, to have access to read any matter sent or received by the user.

5 Use of Social Media, Internet Messaging and Chat Rooms

5.1 Whilst the school appreciates that networking software such as Facebook, Instagram or Twitter provide opportunities for personal expression, the creation of communities, collaboration and sharing, the use of social media, internet messaging and chat rooms must be used with caution and in accordance with our social media policy.

5.2 Avondale tablets and computers are used for educational purposes or in the administration of the school. Activities such as gaming, shopping and your own social networking are not permitted.

5.3 Staff must not communicate directly with students using social media, internet messaging and chat rooms.

5.4 Always be wary about revealing any of your own personal information or school information online.

Avondale may monitor without notice any posts, blogs and other forms of messaging and has the right, if it wishes, to have access to read any matter sent or received by the user.

6 Copyright

6.1 Users must abide by copyright legislation if the intention is to use or publish materials through the internet. The use of online materials for teaching and learning is different from the use of printed and television or audio broadcast materials, which are covered by the Copyright Licensing Agency (CLA) and the Educational Recording Agency (ERA).

6.2 All materials published on the web (irrespective of format) are subject to copyright law and may not be copied or otherwise reproduced without the copyright owner’s permission. Permission may be granted by the owner as stated at their site, or it may need to be obtained directly from the owner. It is insufficient just to acknowledge the source. If Internet materials are clearly labelled as being copyright-free or in the public domain then it may be legally acceptable to use the materials.

6.3 Similar care must be used in copying music, video or music from CDs, CDROMs or DVDs. Possession of the originals does not automatically entitle the user to copy the contents in any format and it may be illegal unless expressly authorised on the media or packaging itself.

7 Use of Personal Laptops on the School Network

7.1 Connecting personal laptops or mobile computing devices to the network is not permitted unless permission has been given by the headteacher. However, you can connect your personal devices to the internet via the school wi-fi. If you choose to do so, this policy will apply to those devices.

7.2 The use of the camera function on any personal mobile device is strictly forbidden at all times. Photographs may only be taken using a school tablet and for marketing or educational purposes, and always with the consent of those being photographed.

7.3 If you bring a personal laptop or other personal computing devices (such as tablets or smartphones) into school, they are entirely your responsibility. If you access the internet whilst in school, it is expected that you will abide by the ethos of this document.

8 Use of Personal Storage Items

8.1 Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.

8.2 Any mobile storage devices such as USB pen drives or external hard discs which are being used to store confidential data must be appropriately encrypted. See note below in reference to data security.

8.3 The need for personal storage devices is eliminated by the appropriate use of OneDrive, which the school provides and expects users to utilise appropriate and effectively.

9 Data Security (including guidelines on creation and security of passwords)

9.1 Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons.

9.2 The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computer Misuse Act 1990.

9.3 Protect yourself by keeping your password private; never use someone else's username and password, even if they ask you to do it.

9.4 It is recommended that passwords are six or more characters long and include at least one numeric or nonalphabetic special character.

9.5 Any mobile storage devices such as USB pen drives or external hard discs must be appropriately encrypted, although great care should be taken with using the devices to ensure that personal, confidential or sensitive corporate data is not taken off-site. (See 8.3)

9.6 Be wary of revealing any of your own personal information or school information online.

9.7 Respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk and would be classed as a direct breach of this policy.

9.8 Your data is your responsibility. Avondale network may review your files and communications to ensure that you are using the system responsibly.

10 Health and Safety

10.1 Protect ICT equipment from spillages by not eating or drinking around it.

10.2 In addition, please read this document in conjunction with the school's Health and Safety Policy document.

11 Equipment

11.1 Installing or attempting to install or storing unauthorised programs of any type anywhere on the network is not permitted.

11.2 Do not damage or disable ICT equipment or intentionally waste ICT resources. This puts your work at risk and reduces the availability of ICT equipment for everyone.

11.3 You should only use the School's printing facilities for printing school-related work, after it has been proof-read for errors and corrected, and you will only print out multiple copies after you have considered alternative methods of delivery, such as Teams.

11.4 You will look after your school issued tablet and ensure it is always kept in its case.

12 Monitoring by the School

12.1 Staff must only access those services they have been given permission to use and they must not access the internet or email for inappropriate purposes.

12.2 Avondale will routinely monitor and audit the use of the internet to ensure compliance with the above policy.

13 Sanctions for Misuse

13.1 As previously stated, on evidence provided, a user may be disciplined by the school. If the above policy is violated, access to network will be withdrawn and you will be subjected to disciplinary action.

13.2 The school reserves the right to discipline any member of staff for actions taken outside of school if they are intended to have an effect on a staff member or they adversely affect the safety and well-being of student and staff members while in school.

13.3 The user's behaviour may be reported to the police.

13.4 If an employee has their network access withdrawn, with or without notice, and wishes to appeal against the decision, this should be done via the grievance procedure as outlined in the staff handbook.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Signature: .....
Name: .....
Date: .....

Pupil Agreement Form: Responsible Use of Information and Communications Technology & Resources

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
13. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
14. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
15. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

16. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
17. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
18. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
19. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
20. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
21. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.
22. ***I will care for my school*** Chromebook and keep it in its protective case at all times.
23. ***I am responsible*** for ensuring my Chromebook is fully charged and ready for school each day.
24. ***I will not install,*** remove, or tamper with software or applications on school ICT equipment, including my Chromebook, without permission.
25. ***I know that personal mobile devices*** (tablets, laptops, etc.) are not permitted in school.
26. ***I know that if I misuse digital*** resources, my access may be revoked.
27. ***I know accidental damage*** to my Chromebook will result in a charge to parents/guardians for repair or replacement.
28. ***I know deliberate damage or reckless handling of my Chromebook will require my parents/guardians to cover the full replacement cost (£220 including VAT).***

For parents/carers

If your parents/carers want to find out more, they can read Avondale's full E-Safety Policy from the school website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.

Agreement & Signatures

I have read and understand the above and agree to use the school's ICT resources responsibly.

Student Name: _____ **Signature:** _____
Date: _____

I have read and understand the above.

Parent/Guardian Name: _____ **Signature:** _____
Date: _____

As the parent of …….

I have read the ‘Pupil Agreement Form’ and these rules apply when my child is using school computers and the Internet.

I have gone through the e-safety guidelines with my child and explained their importance for staying safe online. In the event that children do not follow the school guidelines the school will take appropriate action which may result in one of the following sanctions;

a) Temporary or permanent ban on use of the Internet and Chromebook
b) Additional disciplinary action in line with the school's Behaviour Policy.

I understand that the school will make every reasonable effort to restrict access to all controversial material on the Internet, but I will not hold them responsible for materials my son or daughter acquires or sees as a result of the use of the Internet at school.

I give my permission to Avondale to allow the student named below to use the computers and Internet in the school.

Pupil’s Name:_____ Class: _____

Parent’s Name: _____ Date: _____

Parent Signature: _____