Introduction

Internet Use for Children and Young People with SEN

- Children with SEN are more vulnerable and more at risk than others when using computing equipment:
- Children with ASD may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs do not always understand the concept of friendship and therefore trust everyone implicitly. They do not know how to make judgements about what information is safe to share. This leads to confusion about why you should not trust others on the internet.
- Some children may be vulnerable to being bullied through the internet, or not recognise they are being bullied.
- They may not appreciate how their own online behaviour may be seen by someone else as bullying.
- All school staff will be aware of well-developed strategies to keep pupils safe when using technology, including the internet.
- The policy also addresses legal obligations with respect to copyright and data protection.

Legislation and guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, *Keeping Children Safe in Education 2018*, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department’s guidance on protecting children from radicalisation.

Information system security

1. How will information systems security be maintained?
It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils. Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current. Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption. Wide Area Network (WAN) security issues include:
  - The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Harrow. These industry leading appliances are monitored and maintained by a specialist security command centre.
  - The security of the school information systems and users will be reviewed regularly.
  - Virus protection will be updated regularly.
  - Personal data sent over the internet or taken off site will be encrypted. Portable media may not be used without specific permission followed by an anti-virus / malware scan.
  - Files held on the school’s network will be regularly checked.
  - The computing coordinator will review system capacity regularly.
  - The use of user logins and passwords to access the school network will be enforced.

2. DEFINITIONS

**Undesirable materials**

- Pornographic images or obscene text on internet web sites
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on web sites or in e-mail messages
- Racist, exploitative or illegal material or messages on web sites or in e-mail
- Copyrighted, trademarked and other proprietary materials used without proper authorisation
- There may be other materials that is deemed to be illegal

**Undesirable contacts**

- E-mail messages from unknown or unverified parties who seek to establish a child’s identity and/or to communicate with the child for advertising or potentially criminal purpose

**Unacceptable use**
- Deliberate searching for and access to undesirable materials
- Creating & transmitting e-mail messages that contain unacceptable language or content
- Creating & publishing Internet materials that contain unacceptable language & content

**Adults**
- School teaching staff
- Non-teaching school staff
- Governors
- Parents
- Visitors

**E-mail**
- Pupils are not given their own e-mail accounts on the school system.
- Access in school to external personal email accounts may be blocked.
- E-mails sent to an external organisation by staff should be written carefully and checked before sending, in the same way as a letter written on school headed paper.
- All data e.g. pupil names, date of births etc. must be anonymised across email. For example, when emailing other professionals regarding a pupil, you should never use pupil’s name but use initials instead.
- Email is covered by General Data Protection Regulation (GDPR) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security.

**Published content and the school web site**

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils’ names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. “Over the shoulder” can replace “passport style” photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils’ work or of a team activity. Pupils in photographs should, of course, be appropriately clothed. Images of a pupil should not be published without the parent’s or carer’s written permission. Please see the schools data protection policy for further information.

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils’ personal information will not be published without permission.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
• The school will obtain permission from parents/guardian if they wish to use a pupil’s image on the school website.
• All pupils who feature on videos published on the school website will have permission given to do so from parents/guardians.
• A list of pupils who have permission to be published on the school website/any other media resources will be kept securely in the school office and on the schools network system.

Pupil’s images and work published on the school website:
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
• Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
• Written permission from parents or carers for the use of photographs on the website is requested as part of the annual data collection process.
• Staff will not send pupils images by email.

Social networking and personal publishing
• The school will block/filter access to social networking sites using filtering software.
• Pupils, where applicable, will be advised, where appropriate, never to give out personal details of any kind which may identify them or their location.
• Where applicable, pupils should be taught to understand the risks posed by the internet and how to keep themselves and others safe.
• Staff should understand the risks posed by those who use the internet to bully, groom, radicalise or abuse pupils.
• School leaders are expected to oversee the safe use of technology in school and take action immediately where there are concerns about bullying or a pupil’s wellbeing.
• All staff has a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.
• Following the Keeping Children Safe in Education guidelines 2018, it is the responsibility of all staff to ensure that all children that are accessing the internet in school are doing so through the schools internet and not 3G or 4G domains. This insures that block and filter access is in place when pupils are using the World Wide Web.
• Pupils and parents/guardians will be advised that the use of social network spaces outside school brings a range of dangers for our pupils. Parents are to sign the school policy on ‘Parents Use of Phone and Internet Policy’ when their child first comes to Woodlands school.
• The school’s Social Media for Personal Use policy and Staff Code of Conduct will be given to all staff to read.

Staff
- As part of their induction policy, staff are to read the Social Media for Personal Use policy and sign to say that they have read it.
- Staff are to use school email for work use only.

**TAKING AND STORING IMAGES AND ASSESSMENTS**

- Pupil’s images and assessments, which are stored on school computers, CDs, iPad, the cloud and DVDs, must be accessible exclusively to teaching staff. Pupil’s images and assessments stored on school PC’s must be saved onto staff individual accounts protected by their own password or stored centrally on curriculum server in “Teaching Only”, which is accessible only to school teaching staff. Staff have to keep their password safe and do not share it with other staff.
- All images and assessments to be stored at the end of each academic year on CDs or DVDs and deleted from computer drive and stored in a locked cupboard with access provided only to authorised people.
- Staff must not use their personal equipment to record any images (camera, phone camera, etc.)
- All the images and assessments of the children who left the school will be forwarded to their new school or destroyed.
- If staff need to take home images and assessments of the children to write reports etc. they must use their mobile device which has an individual security code or encrypted pendrives. The school also uses the DropBox official website ([www.dropbox.com](http://www.dropbox.com)). If a member of staff wishes to use the DropBox website to transfer school work they must do so on their own individual account protected by their own password and ensure that its content is not shared with unauthorised users.
- If staff takes their mobile device home (iPad, see appendix i), they must ensure that the security code lock is activated. Each iPad has an individual security code that only the teacher and computing coordinator knows.
- All staff must adhere to the e-safety guidelines that come under the schools device loan agreement (See appendix i) that they must sign before obtaining their mobile device.
- All staff that upload photos on the school evidence for learning app must ensure that there is parental consent given for the children’s photographic assessment evidence to be uploaded on to the app, as per the schools data protection policy.
- In the case of school staff losing their mobile device, they must **immediately** report this to the schools computing coordinator who will then follow the correct procedure in accordance to the schools data protection policy.
- All staff who is using the evidence for learning assessment app should try, when possible, to only upload pictures of the pupil who they are assessing.
- In cases where there are other pupils in the photographs, the staff should ensure that parental consent have been given for all pupils that
are featured in photographs to be uploaded onto the app.

- Please see the schools **Data Protection policy** for more information on our use of photographs and videos.

**Managing filtering**

- The school will work with the Local Authority and London Grid For Learning to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Head teacher or the computing co-ordinator.
- The computing co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- All school staff should be doing all that they reasonably can to limit children’s exposure to the risks from the school’s computing system. As part of this process, all staff should make sure that appropriate filters and monitoring systems in place are working effectively and any problems raise it with the computing co-ordinator. *(Annex C Keeping Children Safe in Education 2018)*

**Staff training**

Woodlands school should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach including PREVENT training. *(Annex C Keeping Children Safe in Education 2018)*

**Unintentional exposure to children of undesirable materials**

It is the school's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the internet. It is recognised that this can happen not only through deliberate searching for such materials but also unintentionally when a justifiable internet search yields unexpected results. To prevent such occurrences the school has adopted the following position:

The use of an Internet provider who offers protection by internet filtering system blocking access to sites which filtering system recognises as unsuitable

In-School protection by:

- Adult supervision of pupils' internet activity with no searching of the internet allowed without a suitable adult present.
- Educating pupils on safe and responsible behaviour when using internet and related technologies;
The application of language and image filtering by appropriate software which is checked and updated on a regular basis by WiBird.

It is part of staff duties under the Prevent strategy all staff should ensure that children are safe from terrorist and extremist material when accessing the internet in school.

No filtering software is fool proof hence filtering software provided by LGFL and WiBird is regularly checked and updated. Any problems in this area that are noticed by staff must be reported to WiBird and reported to the Head Teacher immediately.

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken:

- Pupils, where applicable, should notify a teacher/TA immediately
- The Deputy Head as safeguarding lead should be notified by the teacher/TA
- The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party. This should be reported to the Deputy Head as safeguarding lead where it will be logged.
- The child's parents and/or the School Governors should be notified at the discretion of the Head teacher according to the degree of seriousness of the incident.

Staff must be aware that any accidental or intentional use of language and/or access to inappropriate materials could be reported to the local authorities and may result in disciplinary and/or legal actions. If any member of staff witnesses any incidents or inappropriate use of mobile technology they must report it to the Head Teacher or computing co-ordinator immediately. All incidents will be recorded in a central log. (Please refer to safeguarding policy)

**PREVENT**

- As with other online harms, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups. All staff at Woodlands School are to complete PREVENT training.
- All staff at Woodlands School has a vital role to play in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse.
- In the same way that all staff are to be vigilant about signs of possible physical or emotional abuse in any of their pupils, if you have a concern for the safety of a specific young person at risk of radicalisation, you should report it immediately to the schools safeguarding lead. (DOE: The use of social media for online radicalisation 2015)
Managing video conferencing

Video conferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems.

- The leadership team of the school may choose to use skype for video conferencing, for example for interviewing.
- When doing so, school equipment such as laptops and webcams must be used and no personal webcams.
- All videoconferencing equipment in any room must be switched off when not in use and not set to auto answer.
- The equipment must be secure and if necessary locked away when not in use.
- School video conferencing equipment will not be taken off school premises without permission.
- Responsibility for the use of the video conferencing equipment outside school time will be established with care.
- Unique log on and password details for video conferencing services e.g. skype should be created. Personal accounts should not be used.
- ‘Facetime’ is automatically removed from all classroom iPads unless requested otherwise.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Under no circumstances should pupils have access to staff mobile phones.

Unlawful and illegal use

- All material, which depicts the abuse of children and young people, is illegal. Other illegal materials include race hatred, incitement to violence. These are not exclusive categories. There may be other information that is deemed illegal.

- In the event of receiving an image deemed as illegal or abusive it is imperative that adults make no attempt to investigate the content. A log reference should be made to the safeguarding lead to show that there is suspicion of undesirable material. This log is to protect adults from any suspicion for having potential illegal materials in their possession. It is
possible to accidentally open a link so care must be taken.

**Intentional access of undesirable materials by children:**

- Children must never intentionally seek offensive material on the internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a safeguarding and disciplinary matter and the parents of the children or children will normally be informed.

**Deliberate access to undesirable materials by adults**

- Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious misconduct and disciplinary and/or civil action might arise. The Governors will be advised and the LA consulted. If any member of staff witnesses any incidents or inappropriate use of mobile technology they must report it to the designated safeguarding lead or computing co-ordinator immediately. If any staff believes that the Head Teacher has made deliberate access to undesirable materials this must be reported to the chair of governors immediately.

**Legal considerations**

- It is recognised that all materials on the internet are copyright unless copyright is specifically waived. It is the school's policy that the copyright of internet materials will be respected. Where materials are published on the internet as part of the teacher’s professional duties copyright will remain with the City Council. Internet materials will contain due to copyright acknowledgements for any third party materials contained within them.

**Assessing risks**

- The school will constantly monitor all computer access by both staff and pupils. Any inappropriate content will be reported directly to the Head Teacher.
- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences
of internet access.

- The school will audit computing provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The school and its staff will follow and adhere to the schools ‘PREVENT’ duty and will ensure that all children that are vulnerable to radicalization through the use of the internet are identified to the schools safe guarding officer.

**Handling e-safety complaints**

- Complaints about staff misuse will be referred to the Head Teacher.
- Complaints about the Head Teacher must be reported to the Chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred directly to the designated Safeguarding Lead.

**Guidelines for students and staff using the computer/computing equipment**

- Use your own log in and password, which is kept secret, as by giving your log in details to others you might be giving access to confidential information. Do not leave your workstation unattended when you are logged in.
- Pupils, when allowed to work on a school computer, to use student log in with a restricted access to school intranet to protect other people’s work and sensitive data stored
- All members of staff are responsible for protecting the security and confidentiality of the school network
- Don’t attempt to change any computer, monitor or software settings on any school computer
- Use school computers with care. They are there for everyone to use. Report any misuse or damage of computing equipment to the computing co-ordinator or the Head Teacher.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

**Other relevant policies**

Please see the following policies for further information regarding personal use of the internet
- Safeguarding & Child Protection policy
• Staff Use of Social Media for Personal Use
• Parents policy on use of social media and mobile phones
• Use of Mobile phone policy
• Computing policy
• Data protection policy

References

• Keeping Children Safe in Education 2018
• The Department of Education: The use of social media for radicalisation 2015
• www.gov.uk/government/publications/prevent-duty-guidance
Appendix I:

WOODLANDS SCHOOL

A courageous confident learning community

Device loan agreement

Part of Woodlands School’s Improvement Plan is to maximise the use of computing and to continue to use data to contribute to the effectiveness of the school. Staff members will be provided with a mobile device to use for assessment to assist with this. The Head Teacher has agreed that the mobile device will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time. If, for any reason you loan your device to other members of staff then you must ensure that email notification and pop ups are disabled so that information cannot be intercepted.

As a member of staff to whom a mobile device has been loaned you are required to read and agree to the following terms and conditions that apply while the mobile device is in your possession:

1. The mobile device, and any accessories provided with it, remains the property of Woodlands School and is strictly for sole use in assisting with assessment of pupils in the delivery of the Curriculum.

2. If the mobile device is stolen from an unattended vehicle or a house, you will be responsible for its replacement if it was loss/stolen due to recklessness e.g leaving the ipad in view in a car.

3. Treat the mobile device with due care and keep the device in good condition, ensure that it is kept in the protective cover, do not leave the device unattended in class without being secured and out of sight.

4. I agree to back up my work on a regular basis in the cloud space (see help sheet). I understand the school will not accept responsibility for the loss of work in the event of the device malfunctioning.

5. I agree to only use software licensed by the school, authorised by the Head Teacher and installed by the school’s computing staff (e.g computing co-ordinator and Wibird)

6. I agree to not leave my device logged in and unattended at any location, including at home. I also agree to not permit persons other than school staff to
have access the device and the potentially sensitive material it provides access to.

7 Should any faults occur, I agree to notify the school’s computing staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or any one other than computing staff, attempt to fix suspected hardware, or any other faults.

8 I agree that home Internet access is permitted at the discretion of the Head Teacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.

9 I agree to adhere to School and LA policies regarding the following, updated as necessary:
   • Safeguarding & Child Protection
   • E-Safety
   • Staff Use of Social Media for Personal Use
   • Data protection
   • Health and safety

Personnel Details

I have read and agree to be bound by the terms and conditions set out above.

Staff Name:

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