USING SOCIAL MEDIA AND TECHNOLOGY SAFELY AT RADLETT LODGE SCHOOL (GUIDELINES FOR STAFF)

At Radlett Lodge School we have a duty and responsibility to protect the children in our care from being exposed to material that compromises their safety or could potentially cause them harm by creating fear or anxiety. The use of information and communication technologies (ICT) including the Internet has developed over the past 25 years and now involves every pupil And member of staff. While these advances bring many benefits, such Powerful technologies have their dangers. It is for this reason that we have drawn up these guidelines for staff who will be supervising the pupils using these technologies.

It is the aim of RLS not to block access to these technologies merely to put in place a number of safeguards that will protect the pupils. A key part of this protection will be the teaching of online safety to pupils so they can recognise and manage the risks themselves during use in school, residential unit or the home. (See RLS Computing policy). These guidelines do not provide detail on this element, rather they define the procedures in place and the expectations for staff.

It is important that these guidelines are read and understood by staff as they are responsible for supporting pupils in using these technologies and any misuse / or failure to follow procedure could result in disciplinary procedures.

Online Safety Plans

We aim for each pupil to have an individual online safety plan. School and residential staff work on these together to ensure consistency in both settings. Plans are based on individual pupil use of ICT, internet and social networking and will take into account any individual current safeguarding issues for the pupil. UNTIL A PUPIL HAS AN INDIVIDUAL ONLINE SAFETY PLAN (that specifies independent access) ALL INTERNET USE WILL BE SUPERVISED.

Use of internet

Due to the nature of the difficulties of the pupils in this school, staff have to accept full responsibility for the pupils' use of the internet when they are supervising them.

Pupils may use search engines whilst being supervised by staff and as part of planned lessons / activities.

Use of mobile phones

If staff are aware that a pupil has brought their own mobile phone into school then they must inform the Principal and online safety officer.

The Principal has the discretion to make a decision on whether a child should be allowed a mobile phone in school and if they are how it should be used. This decision will be made on an individual basis and guidance passed on to staff if required.

Pupils are not allowed to take photos on their own mobile phone.

Use of email

Pupils may be given a secure email account. The Computing Curriculum Leader and/or online safety officer will make class teachers and residential seniors aware of who these pupils are.

PUPILS MAY ONLY USE AUTHORISED EMAIL ACCOUNTS WITHIN SCHOOL.
Unless a pupil's online safety plan details that pupils may send / receive emails independently STAFF SHOULD SUPERVISE PUPILS WHILST THEY SEND AND RECEIVE EMAILS.

Pupils should be taught about safe rules related to receiving emails and staff should be vigilant to recognising any signs of distress in pupils that may indicate they have received an offensive email.

Social Media Tools

Social media tools can include websites such as blogs, Wikis, social networking and video sharing sites. Sites such as Facebook, MySpace, Twitter, YouTube and Flickr have become everyday forms of communication for both adults and children. Whether accessed through a computer or mobile phone, they help us stay in touch with friends and family members, share photos, watch videos, play games and even organise events and campaigns.
However social networking and media sites can have risks. They have changed how we communicate and this can lead to people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and abuse children. The boundaries between the "real" world and the "virtual" can become blurred and this can have potentially serious consequences for staff, parents/carers and children who may not be aware of the risks behind everyday online activity.
Online social media tools can also be excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with pupils and the wider community. The positive use of social media and Information and Communication Technology (ICT) within schools and settings for curriculum and learning is encouraged. However it is essential that their use is carefully considered in advance, in order to ensure all members of the school community are kept safe.

Social networking sites (e.g. Facebook, Twitter, Bebo, MySpace) and specific social networking apps (e.g. Vine micro-videos and Snapchat) can be made available for specific pupils to access via the NAS network and wifi accessible mobile devices (not 3G/4G).

Pupils may only be given access to social networking once they have an individual online safety plan in place and if it is being taught as part of their curriculum or through specific leisure time (e.g. for residential or Post 16 pupils).

The individual online safety plan will detail the pupil's current knowledge / awareness of online safety, the main aims, potential risks, key priorities and strategies or control measures. This is to ensure sufficient measures are put in place to enable the pupil to learn about online safety alongside using such a tool.

NO PUPILS SHOULD USE SOCIAL MEDIA TOOLS WITHOUT ADULT SUPERVISION OR WITHOUT AN ONLINE SAFETY PLAN BEING COMPLETED.

The teaching of the use of social media and related safety issues will be taught through the Citizenship, PSHE and Computing schemes of work.

Use of wireless devices (e.g. iPads)

The school now has a large number of iPads for pupil use. Wifi is available to access the internet on such devices. A filtering system is in place whether using the NAS network or the wifi network.

Pupils are currently not allowed to use 3G/4G activated BYO devices. When using wireless devices staff and pupils must follow same rules as described in previous sections.

Pupils may bring in their own iPads for communication purposes. This should be agreed with the Principal or Deputy Principal and the Speech & Language Therapist.

All classes have an allocated amount of iPads. In the lodge each pupil has their own iPad, labelled and identifiable with a photo or name of the young person on the home screen.

Pupils and staff are not allowed to take photos or video of other pupils on their own iPads without the consent of the parents/carers.

iPads that go home with pupils should be checked routinely before the end of the school/lodge day to ensure there is no unauthorised footage of others.

iPads should not be taken off site with photos of children stored on them. However, they may be used to take an image of a pupil before an educational visit as part of the risk assessment. Photos may be taken whilst on the visit.

Any member of staff needing to borrow an iPad overnight make sure all photos and video have been downloaded to the school network and deleted from the iPad.

Reporting incidents of misuse / online safety concerns.

The schools online safety officer and Principal should be informed of any incidents of misuse or online safety concerns. This includes if a pupil accessed something that should have been blocked by the NAS filtering system.

ALL STAFF ARE RESPONSIBLE FOR REPORTING ONLINE SAFETY INCIDENTS

The online safety officer will keep an incident log book that should be completed for each incident.

The online safety officer and principal will decide whether or not the incident involved any illegal activity and will follow up using the appropriate channels / procedures as detailed in the NAS policy and Hertfordshire advice (Flowchart to support decisions related to an online safety incident).

Emergency safeguarding procedures

Due to the filtering systems in place it is highly unlikely that any material deemed inappropriate would not be blocked. However, in the unlikely event that material is accessed the following steps can be taken in order to stop access:

1. The online safety officer or designated senior person can change the level of filtering. This will immediately block access to specific sites.
2. The online safety officer or designated senior person can change the wifi password. This will immediately disable any wifi users who will need to enter the new password in order to regain access.
3. Any staff member can shut down the Wi-Fi connection by pressing the button marked with a red X in the resources cupboard. This will close down all internet use immediately.

The online safety officer, SLT and designated senior staff on duty will be provided with login details for changing the passwords and filtering and will be shown how to do this.

A sealed envelope containing details of the passwords for changing the filtering levels and Wi-Fi passwords will be kept in the lodge office and the Deputies office if for any reason a senior with the details is not on site. Staff will be told where to find these in each location and will inform the senior by telephone or on their immediate return to school.

Other policies to be read in conjunction with these guidelines:

- NAS “Acceptable Use of ICT” Policy (see policies file).
- NAS Schools Online Safety Policy
- ICT/Computing Policy (Radlett Lodge School)
- Early Years and Post 16 Policies.

Please ensure you have understood these guidelines. You are responsible for supervising pupils safely using Information Communications technology.
If you have any questions please see the ICT Curriculum Leader

After reading these guidelines staff please sign to say that you have understood and are willing to accept responsibility for supervising pupils using the internet. Some staff may not feel confident using such technologies or may be unwilling to accept responsibility for supervising use, and may choose not to sign these guidelines. Only staff who have signed these guidelines, will be allowed to supervise pupils using these technologies

I have read and understood
USING SOCIAL MEDIA AND TECHNOLOGY SAFELY AT RADLETT LODGE SCHOOL
(GUIDELINES FOR STAFF)

Signed: ……. Date: …….

Name: ……..

I have read and understood the policies and procedures listed below:

- NAS "Acceptable Use of ICT" Policy (see policies file).
- NAS Schools Online Safety Policy
- Computing Policy (Radlett lodge School)

I have been shown where to find the 3rd emergency measure for shutting down the internet in case of a safeguarding emergency.

Signed: ……. Date: …….

Name: ……..