



Oakgrove

Acceptable Use Policy

The aims of the Acceptable Use Policy are to:-

- Ensure that children benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that Internet use in school is a resource and privilege. If the terms are not met then the privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and the personal items that are brought into school.

Oakgrove School will develop the learning environment to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our school's vision.

General

- Virus Protection software is used and updated on a regular basis.
- A member of staff is appointed as responsible for the school's e-safety.

Children's access to the Internet

Oakgrove School use a "filtered" Internet Service, which will minimise the chances of children encountering undesirable material. Oakgrove will normally only allow children to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to children, the expectation we have of children. Teachers will have access to childrens' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.

Expectations of children and staff** using the Internet

- All children are expected to read and agree the Internet Agreement.
- At Oakgrove, we expect all children and staff to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes materials they choose to access, and language they use.
- Children and staff using the World Wide Web are expected not to deliberately seek out offensive materials. Should any children or staff encounter any such material

accidentally, they are expected to report it to the ICT leader, so that the Service Provider can block further access to the site.

- Children are expected not to use any rude language in their email communications and contact only people they know or those the teacher has provided. They have been taught the rules of etiquette in email and are expected to follow them.
- Children must ask permission before accessing the Internet and have a clear idea why they are using it.
- Children and staff should not access other people's files unless permission has been given.
- Computers should only be used for school work and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No program should be brought in by pupils from home for use in school although staff can seek permission from the Head. This is for both legal and security reasons.
- Homework completed at home can be brought in on a memory stick, but this will have to be virus scanned by the class teacher before use.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Children and staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to internet resources. They will also come under general discipline procedures of the school which comprises an escalating set of measures including a withdrawal of privileges.
- Uploading and downloading of non-approved software will not be permitted.

School Website

- The website will be regularly checked to ensure that there is no content that compromises the safety of children or staff.
- The publication of children's work will be decided by the teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

Personal Devices

Staff and children may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of the SLT or ICT Leader.

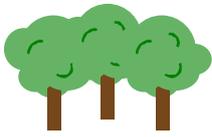
Inappropriate use is in direct breach of the school's acceptable use policy.

Pupils must not use their own technology in an attempt to contact members of school staff.

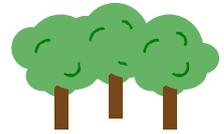
Sanctions

Persistent misuse of the internet by pupils will result in reducing access to the Internet. Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Head Teacher. Parents will always be notified.

**A staff code of conduct re: use of ICT, was discussed at a staff meeting in March 2013, and was added to the Acceptable Use policy and reviewed in Summer 2013, and annually thereafter.



Oakgrove Staff Code of Conduct for ICT



The purpose of the code of conduct is to provide guidance about safer working practice, keeping my personal and private lives separate, keeping myself safe when using electronic media and adopting responsible behaviour that should prevent me from putting myself and my career at risk.

This document refers to professional working relationships with colleagues, children, young people, parents / carers and volunteers.

I Will Not:

- o Give my personal details to children/young people. This includes mobile phone numbers, details of blogs, details of personal websites, social networking accounts, passwords, PIN numbers, Log in Details
- o Give my passwords and Log In details to anyone
- o Use my personal mobile phone to communicate with children/young people except in genuine emergencies.
- o Make available my personal details on a social network site with children/young people. I am aware that belonging to a group may give a back door to my page
- o Add/allow a child/young person to join my contacts/friends list
- o Use the internet or web-based communication to send messages to children/young people un-related to school
- o Use Social Networking sites to discuss children and young people, using their name or initials
- o Use my personal e-mail address in any communication with children and young people
- o Tick the 'remember me' box when using password protected internet sites in school
- o Retain pupil/family contact details for personal use
- o Produce images of children and young people unless appropriate permission has been sought
- o Retain images for personal use or move them for personal use
- o Use school information systems for private purposes without the permission of the Headteacher or designated alternate
- o Install any additional hardware or software without the permission of the Headteacher or designated alternate
- o Upload or download inappropriate or illegal material, nor assist young people in this process

I Will:

- o Only use my mobile phone in line with school policy during directed time
- o Always anonymise my mobile phone number where possible where my phone is used to contact parents, carers or volunteers
- o Switch off any blue tooth visibility
- o Password – protect, switch off and lock my technology when it is not in use
- o Ensure that all written communications are compatible with my professional role
- o Remember that on-line conversations are written documents and should be treated as such

- o Store images of children/young people in the secure network space specified by the school and
- o Delete such images from the device as soon as they have been stored whether using my own digital camera (with the permission of the Headteacher) or that of the school
- o Remove any contact details of children/young people /parents/carers/volunteers from a mobile device once the activity is complete. This includes school equipment and my personal mobile if permission for its use has been granted
- o Respect copyright and intellectual property rights

I Will Consult the Headteacher if:

- o I have an existing social relationship with a child/young person/parent/carer / volunteer outside school which leads me to communicate with them using technology
- o I have an existing social relationship with a child/young person/parent/carer/ volunteer outside school which leads me to play on-line games with them

I understand the advice listed below:

Oakgrove recommends that you:

- o Set your privacy settings at a maximum for any social network site/image storage etc.
- o Make sure that any information that is about me that is publicly available is accurate and appropriate to my professional role
- o Are mindful about how you present yourself when you are publishing information about yourself or having conversations on-line
- o Assume that **any** information that you post is publicly available

Additional Requirements:

Please tick

- I am aware that I must not behave in a way that could suggest that I am trying to develop a personal relationship with a child known to me through my professional role
- I have read the E-Safety Safer Working Practice Guidelines produced by Stockport Safeguarding Children Board
- I will report any incidents of e-safety regarding children/young people to the Designated Child Protection Officer (Helen Hammersley or Rob Metcalfe) in school
- I am aware that activities I undertake within my private life using technology may bring the profession/establishment into disrepute
- I understand that the headteacher may ask to view my school equipment at any time

- I accept responsibility for the use of youtube for teaching and assembly purposes and agree to ensure all images viewed are appropriate for use in school, so far as I am able
- I agree to not discuss any Oakgrove child by name or other identifiable description (e.g. class name or initial) on any social networking site
- I agree to keep my personal mobile phone in the staffroom or locked in a class store room during directed time (unless in exceptional circumstances and in agreement with the Headteacher). Office based staff to keep mobile phones in office cupboards/drawers during times when pupils are in school.

I have read and understand the above Code of Conduct.

Signed:

Full Name:

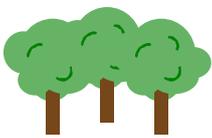
Date:

Received By: Helen Hammersley

Role: Deputy Headteacher and designated safeguarding child protection officer

Date:

Original copy to be stored in personal file



Oakgrove eSafety Pupil Code of Conduct



- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open or delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
 - ✓ I will not use any ICT device to contact members of school staff.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Name

Date