Overfields Primary School

E Safety Policy

Updated: **September 2016**

Author: **Mrs Tracy Watson**

E- SAFETY POLICY & ACCEPTABLE USE AGREEMENTS

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Overfields Primary with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Overfields Primary
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students

The e-Safety Policy is part of many different schools policies including the ICT Policy, Child Protection Policy, Anti-Bullying and School Development Plan and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship. The e–Safety Policy and its implementation will be reviewed annually.

- The E-Safety Coordinator is Mrs Watson, who is also the Designated Child Protection Lead and Headteacher.
- The E-Safety Governor is Pauline Jackson.
- Technician services are provided through a service level agreement with One IT

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups:

Role	Key Responsibilities

Headteacher, E-Safety Co-ordinator/ Designated Child Protection Lead	• To take overall responsibility for e-safety provision
	• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (EIS)
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant
	• To ensure that e-safety education is embedded across the curriculum
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To communicate regularly with the designated e-safety Governor to discuss current issues
	• To keep up to date with e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	• To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network technician)

Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. To support the school in encouraging parents and the wider community to become engaged in e-safety activities

Role	Key Responsibilities
ICT Technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology(including, extra-curricular and extended school activities) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand and adhere to the Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents/carers	• to support the school in promoting e-safety • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to consult with the school if they have any concerns about their children's use of technology

Teaching and learning

Why is Internet use important?

- The Internet use is a necessary tool for learning, it is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with R& C LA and DfE;
- access to learning wherever and whenever convenient

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The IT Technician will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

- Staff will only use official school provided email accounts
- Access in school to external personal email accounts may be blocked.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published or where pupils' images are used for publicity purposes.

How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised on security and privacy online. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with Redcar & Cleveland Local Authority and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Head teacher.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, the Police or CEOP
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Staff Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the Pupil Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the school's network will be made aware of the schools acceptable use policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Foundation Stage Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cleveland Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- All staff will follow 'Response to an Incident of Concern'

- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police

How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

Pupils Use of Personal Devices

- The use of mobile phones and other personal devices by pupils in school is not permitted.
- School staff may confiscate a phone or device and put it into the school office for safe keeping until the end of the school day.
- Any phones brought to school by pupils will need to have a letter from parents which states school accept no liability for damage/theft of a device stored in school.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Head teacher in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- E-Safety rules will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Head teacher and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents through the school website.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Overfields Primary School - Staff Acceptable Use Agreement / 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 staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Watson , Overfields Primary School e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will not install any hardware of software without permission of ICT coordinator. I understand that any hardware and software provided by school for staff use can only be used by members of staff and only for educational use.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher.
- I will not keep professional documents which contain school related sensitive or personal information on any personal devices.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and will be made available to the ICT coordinator/ Head teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should contact the school office to communicate with the parent. In exceptional cases and where there is no alternative but to use their own devices, staff will hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Staff Signature

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

Signature …….…… Date ……

Dear Parents/Carers

Use of the internet in school

As part of the school's ICT programme, we offer pupils supervised access to the internet. Various projects have proven the educational benefits of internet communication access, which enable pupils to explore a wide range of information sources, and communicate and collaborate with other learners throughout the world. Although there are concerns about children having access to inappropriate material via the internet, the school takes a range of measures to minimise these risks. A filtering system is in operation, which restricts access to inappropriate materials, and this is supplemented by an internet safety programme for all pupils, teaching the safe and appropriate behaviours to adopt when using the internet, forums and other technologies.

Overfields Primary School has developed a set of guidelines for Internet use by pupils. These rules are displayed next to all computers, are included in the consent form and kept under constant review. Before we allow pupils to use the internet, we require parental permission. If you consent to your child to having access to the internet within school, please return the completed form to school as soon as possible.

Overfields Primary Responsible Internet Code for Pupils

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will only use ICT in school for school purposes
- On a network, I will use only my own login and password, which I will keep secret.
- I will not look at or delete other people's files. I will not change any settings on the computer systems.
- I will not bring memory sticks or USB devices into school without permission. I know that the school may check my computer files and may monitor the Internet sites I visit.
- I will ask permission before entering any Web site, unless my teacher has already approved that site.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or share 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 engage in conversation or dialogue with other outside users on the Internet without permission or supervision from my teacher. I will never arrange to meet someone myself.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- 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 e-Safety.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet, computers or school devices.

I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and although the school have done their best to guarantee that unsuitable material will never appear on a school computer the school cannot accept liability for the material accessed. I have discussed the school rules on internet use with my child.

I grant permission for my child _____to use the Internet

Parent's signature _____ Date: ___/___/___

Child's signature _____ Date ___/___/___