

# E-SAFEGUARDING POLICY



**BASED ON THE DONCASTER LA APPROVED POLICY  
GOVERNORS APPROVED POLICY SEPTEMBER 2015  
TO BE REVIEWED NOVEMBER 2017**

**WAVERLEY PRIMARY SCHOOL  
DATED NOVEMBER 2016  
(REVIEWED: ANNUALLY)**

<b>PERSON RESPONSIBLE FOR POLICY:</b>	<b>DIANE HUMPHREY</b>
<b>APPROVED:</b>	<b>DATE: NOV 16</b>
<b>SIGNED:</b>	<b>ROLE:HEADTEACHER</b>
<b>SIGNED:</b>	<b>SHARON ROW - COG</b>
<b>TO BE REVIEWED:</b>	<b>DATE: NOV 17</b>

# E-SAFEGUARDING POLICY

## Waverley Primary School E-Safeguarding Policy

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Waverley Primary we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, whiteboards, digital video equipment; and future resources including tablets, webcams etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

### Roles and Responsibilities

As e-Safeguarding is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safeguarding co-ordinator in our school is Michelle Teale who has been designated this role as a member of the senior leadership team. In addition, Michelle has undertaken 'thinkyouknow' training and is available to give

# E-SAFEGUARDING POLICY

advice to staff where necessary. All members of the school community have been made aware of who holds these posts. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Doncaster LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafeguarding co-ordinator regarding the teaching of e safety issues.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour (including the anti-bullying) and PSHCE policies.

## **E-Safeguarding Staff Training**

- Staff receive information and training on e-Safety issues through the coordinator at staff meetings where necessary.
- Staff will annually receive e-Safeguarding training. (Doncaster LA e-safety officer).
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safeguarding and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart).
- New staff will receive information on the school's acceptable use policy as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons and to consistently remind children explicitly about safe use of the internet at all opportunities.

## **Managing the School e-Safeguarding Messages**

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- The e-safety policy is available on the school website.

## **E-Safety in the Curriculum**

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safeguarding curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if

# E-SAFEGUARDING POLICY

they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- The school will send out relevant e-safeguarding information for parents/carers through newsletters and the schools website.

## E-Safeguarding Information for Parents/Carers

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child.
- Parents/ carers who refuse consent for images of their child being taken/ used in the public domain (e.g., on school website.) must do so in writing.
- The school website contains useful information and links to sites like Thinkuknow, Childline and YHDFL parents' page.
- At times the school will deliver information meetings for parents on e-safeguarding and also write to parents regarding specific e safety issues such as use of 'Facebook'

## Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safeguarding Policy.
- Adult users are provided with an individual network and email and future Learning Platform log-in username.
- Pupils are provided with individual and email log-in usernames and passwords.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think a password has been compromised or someone else has become aware of it, report this to the ICT coordinator.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems (and/or Learning Platform,) including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

## Data Security

The accessing of school data is something that the school takes very seriously. The school follows the appropriate guidelines.

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/pupil data.

# E-SAFEGUARDING POLICY

## Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the DMBC ICT filtering is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

## Infrastructure

- Doncaster Local Authority has a monitoring solution where web-based activity is monitored and recorded.
- School internet access is controlled through the LA's web filtering service. Please contact the IT helpdesk at the Local Authority for further details.
- Waverley Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act , The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safeguarding co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility or the network managers to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ICT coordinator/technician for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT coordinator/technician.

# E-SAFEGUARDING POLICY

## E Mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- E-mail sent to an external organisation should adhere to accepted rules of network etiquette in relation to the use of appropriate language and not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

## Publishing Pupil's Images and Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways: (Refusal of consent must be given in writing.)

- On the schools website and planned Learning Platform.
- In the schools prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/transmitted on a video/webcam.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity.
- Appropriate images taken by staff with school equipment and personal digital equipment such as mobile phones and cameras, should be transferred to the schools network and deleted from the device. (Personal equipment requires the express consent of the Headteacher)

Pupils' full names will not be published alongside their image. Email and postal addresses will not be published.

## Photographs Taken by Parents/Carers for Personal Use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention.

## Storage of Images

- Images/films of children are stored on the schools network and should be deleted when those children leave the school.
- Rights of access to this material are restricted to the staff and pupils within the confines of the school network.

## Social Networking and Personal Publishing

# E-SAFEGUARDING POLICY

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However we accept that some pupils will still use them; they will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites. (Staff Code of Conduct)

## Mobile Technologies

Many new and existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside school. Some now offer open access to the internet and therefore open up risks associated with unregulated internet access. Emerging technologies will be examined for educational benefit and the risks assessed before use in school is allowed.

- The school allows staff to bring in personal mobile phones (**only to be used during their own time**) and devices for their own use and during their own time. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school; any child that needs to contact their parents will be given access to a school phone. Any phones that are brought in will be looked after by the class teacher until the end of day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of any inappropriate messages between **any** members of the school community is not allowed.

## Community Use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety. E.g. Used for adult or family learning courses.

## Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor DMBC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

# E-SAFEGUARDING POLICY

## Handling e-safety Complaints

- 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.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator.
- Depending on the seriousness of the offence; investigation by the Headteacher/ LA may involve immediate suspension, possibly leading to dismissal and involvement of the police for very serious offences.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Should there be any issues or concerns please contact the e safeguarding / ICT subject leader, the Headteacher or the governor responsible for ICT.

# E-SAFEGUARDING POLICY

## **Waverley Primary School Staff, Governor and Visitor 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 Michelle Teale, school eSafeguarding coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- 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 only use the approved, secure email system(s) for any school business.
- 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 or Governing Body.
- I will not install any hardware or software without permission of the Headteacher and ICT coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with 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 Headteacher.

# E-SAFEGUARDING POLICY

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- 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.

## School Equipment

I accept that when school laptops, digital cameras etc. are taken home, they must be covered by the householder's home contents insurance policy.

I understand that if it is necessary to leave school equipment in the car for a brief period (not overnight) it must be out of sight and the car must be locked.

## User Signature

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

Signature ..... Date .....

Full Name .....(printed)

Job title .....

## Waverley Primary School

Douglas Road, Balby, Doncaster DN4 0UB

Telephone **01302 853326** Fax 01302 310753

Email [head@waverley.doncaster.sch.uk](mailto:head@waverley.doncaster.sch.uk)

Headteacher **Mrs D J Humphrey** BA (Hons) PGCE NPQH



Dear Parent/ Carer,

ICT including the internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safeguarding rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school to arrange an appointment.

# E-SAFEGUARDING POLICY



## Parent/ carer signature

We have discussed this and .....(child name) agrees to follow the eSafeguarding rules and to support the safe use of ICT at Waverley Primary School.

Parent/ Carer Signature .....

Class ..... Date .....

## Waverley Primary School Pupil Acceptable Use Agreement/e-Safeguarding Rules

### Using the Computers

- ☺ I will only use ICT in school for school purposes.
- ☺ I will not tell other people my ICT passwords.
- ☺ I will only open/delete my own files.
- ☺ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

# E-SAFEGUARDING POLICY

- ☺ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ☺ I will only use my class email address or my own school email address when emailing.
- ☺ I will only open email attachments from people I know, or who my teacher has approved.

## Using the Internet

- ☺ I will ask permission before using the internet.
- ☺ 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 this is part of a school project approved by my teacher and a responsible adult comes with me.
- ☺ 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.
- ☺ I will not complete and send forms without permission from my teacher.
- ☺ I will not give my full name, home address or phone number when completing forms.

## Using email

- ☺ I will ask permission to check my email.
- ☺ I will only use my class email when emailing.
- ☺ I will only email people I know or who my teacher has approved and will not open attachments.
- ☺ I understand that email messages I send or receive may be read by other people.
- ☺ I will immediately report any unpleasant messages sent to me.
- ☺ I will not give out my own details such as my name, phone number or home address.
- ☺ I will not arrange to meet someone outside school hours.

## Flowchart for responding to e-safeguarding incidents at Waverley Primary School.

# E-SAFEGUARDING POLICY

## Flowcharts for Managing an E-Safeguarding Incident

