Donington Primary School E-Safety Policy

Why is internet use important?

The educational benefits of internet access far outweigh the possible risks and good planning and management will ensure appropriate and effective pupil use. Whilst regulation and technological solutions are very important their use must be balanced by teaching pupils to take a responsible approach, and this forms an essential part of the school's e-safety provision.

How will the internet provide effective learning?

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the schools management of information and business administration systems. Internet access provides many high quality teaching and learning resources, some free, some subscription, as well as providing huge potential for research.

How will internet access be authorised?

Pupils' home school agreement will include the Rules For Responsible Internet Use which needs to be signed by pupils, parents/guardians and returned to school at the beginning of Reception and the beginning of KS2, or when a new pupil starts at the school.

Internet access will be granted to a whole class or individuals as part of a scheme of work, after suitable education in responsible internet use. Older pupils may carry out their own internet searches for research purposes and should know how to conduct searches safely and what to do if they come across something unsuitable.

Pupils' entitlement to use the internet is based on their responsible use of it. Irresponsible use may result in this privilege being removed.

How will the school ensure internet access is as safe as is reasonably possible?

Levels of access and supervision will vary according to pupil's age and experience.

The school will use a Core Services Provider approved by Lincolnshire County Council. The provider manages website/internet filtering and email spam filtering. This is designed to filter out material found to be inappropriate for use in the education environment.

If staff or pupils discover unsuitable sites, the URL address and content will be reported to the head teacher and logged in the 'ICT Reporting Book'. It will be reported to the Core Services Provider via the ICT co-ordinators.

The school will work in partnership with parents, the LA and Core Services Provider to ensure systems to protect pupils are renewed and improved and are effective in practice.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Methods to identify, access and minimise risks will be reviewed regularly by ICT co-ordinators.

How will publishing on the web be managed?

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The point of contact on the school website should be the school address, school email and telephone number. Staff or pupils' home information will NOT be published.

Photographs used on the website must not identity individual pupils. Group shots or pictures taken over shoulders will be used where possible and other carefully selected shots (not passport style images).

Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Permission from parents/carers will be obtained before photographs are published on the school website. Parents will be notified of their right to refuse to allow any pictures of their child to be shown.

Where audio and video are included, the nature of the items uploaded will not include content that allows the pupils to be identified.

Protecting personal data.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
Personal data must be stored on a password-protected laptop or encrypted storage device (e.g. USB memory stick).

How will e-mail be managed?

Pupils may only use approved e-mail accounts on the school system. Whole class or group email addresses should be used at KS1 and monitored accounts at KS2, where incoming and outgoing messages are checked and authorised by the teacher before sending or receiving thus all pupils' emails will be treated as 'public').

Pupils should use email in an acceptable way (being polite and considerate), and must immediately tell a teacher if they receive offensive or distressing messages.

Pupils must make sure they do not reveal any personal details about themselves or others in any online communication, or arrange to meet anyone they meet online.

Information will be provided to parents explaining how pupils can access their accounts from home.

Social networking and mobile phones.

Social networking sites and personal emailing such as Bebo, MSN, Facebook, Hotmail, Yahoo mail, blogs etc are NOT allowed to be accessed by pupils in school.
Staff may use such sites that are allowed by the Core Services Provider filtering system but only when not teaching lessons.

Any digital communication between staff and pupils or parents (email/chat) should be professional in content.

As part of the school's e-safety education programme pupils and parents will be advised that they are inappropriate for primary aged children, pupils in KS2 will be taught about the potential risks and how to keep personal information safe. The purpose of this is to acknowledge (although not condoning) the reality that some children may already have access to social networking sites by this age.

Each year group will have specific ICT/PHSE lessons dedicated to e-safety, as well as follow up assemblies.

Pupils are not permitted to use or carry mobile phones within school. If a parent wishes a child to carry a mobile phone to and from school, the phone should be handed into the school office for safe keeping upon arrival to school. However, appropriate use of mobile phones will be taught to pupils as part of PSHE. Staff may use them only outside lessons, unless contacting the school when on a trip/course.

How will staff and parents be informed about e-safety?

All staff will have access to this E-Safety Policy, and its importance explained with relevant training given and they will sign the ICT Code of Practice for Teachers.

The e-safety co-ordinators will provide advice/guidance/training as required and keep up to date on relevant issues.

All staff should take part in e-safety training provided by the LA/National Governors Association or other relevant organisations.

The school will seek to draw attention to the schools School E-safety Policy and provide information and awareness of key e-safety issues to parents/carers through newsletters, the school website and in the school's prospectus.

How will pupils be informed about e-safety and evaluating content?

E-safety education will be provided in the following ways:-

- A planned e-safety programme should be provided as part of ICT/PSHE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technology in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies, including understanding the need for acceptable use, how to stay safe online and responsible use.
- Rules for internet use will be posted in all rooms where computers are used.

How will complaints be handled?

Responsibility for handling incidents will be given to the head or delegated as the need arises.

Any complaint about staff misuse must be referred to the head teacher and then to the Chair of Governors. Any illegal apparent or actual misuse will be reported to the head, or the police, as appropriate.

Complaints about misuse of the internet in school by pupils must follow the most relevant schools policy (i.e. Behaviour, Anti-Bullying, Racism, Health and Safety).

Monitoring and reviewing

This policy will be monitored annually by the governors and will be reviewed as the need arises or at the review date given.

Agreed by staff

Agreed by governors

Review date

Named E-Safety Governor – Mr Rob Cole 9th July 2014
Named Member of Staff – Mrs Marina Faulkner 9th July 2014