FINEDON INFANT AND FINEDON MULSO CE VA JUNIOR SCHOOLS'

E-Safety Policy

The Federated Governing Body of Finedon Infant and Finedon Mulso CE VA Junior Schools formally adopted this policy at a meeting held on 8th October 2014.

Signed:..

Chair of Governors

Signed:..

Head Teacher

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)

1. Introduction and Overview

E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

> *"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.*
> *"To ignore e-safety issues could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."*
> From: Safeguarding Children in a Digital World. BECTA 2006

Roles and Responsibilities:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Role	Key Responsibilities
Headteacher and Senior Leaders	• To take overall responsibility for e-Safety provision • 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 be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Leader • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. system administrator). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements.
The E-safety leader	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the

	curriculum. • Liaises with school ICT technical staff / support. • To communicate regularly with SLT and the designated e-Safety Governors / committee to discuss current issues, review incident logs and filtering / change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident. • To ensure that an e-Safety incident log is kept up to date. • Facilitates training and advice for all staff. • Is regularly updated in 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
Teachers / teaching assistants.	• 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 where relevant) • 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. • To inform the E-Safety leader if they need training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
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 – Appendix 1 • 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 adhere to the acceptable use agreement with regard to these devices • To report any suspected misuse or problem to the e-Safety leader. • To maintain an awareness of current e-Safety issues and guidance e.g. through training. • 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, sign and adhere to the Student / Pupil Acceptable Use agreement – Appendix 2 • 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 and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the 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 and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images – Appendix 3 • 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 out of school.

2. Teaching and learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- As part of the computing curriculum, all year groups cover digital literacy units that focus on different elements of staying safe on line. These units include topics such as how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning

The Pupil e-Safety curriculum covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;

3. Managing the ICT infrastructure - Internet access, security (virus protection) and filtering

At Finedon schools our network is securely run from the Junior school and we ensure that the schools:

- Has educational filtered secure broadband connectivity through Surf Protect.
- The filtering system blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to the ICT administrators.
- Ensure network health through use of anti-virus software and network set-up so staff and pupils cannot download executable files;
- Use secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Are vigilant in the supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensure all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensure pupils only publish within an appropriately secure environment : the school's learning environment, website or blogging sites.
- Require staff to preview websites before use [where not previously viewed or cached]
- Plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search.
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Inform all users that Internet use is monitored;
- Inform staff and students that that they must report any failure of the filtering systems directly to the system administrator.

  - Our system administrator(s) logs or escalates as appropriate to the Technical service provider.
  - Make clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
  - Provide advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents

- **Network management (user access,backup)**

At Finedon Schools we:

  - Use individual, log-ins for all users.
  - Use guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - Use teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful – Smart Sync (Juniors only);
  - Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, Finedon schools:

- Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 1 they are also expected to use a personal password;
- Make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Key members of staff, particularly those that work across both the infant and junior school, have access to the staff shared area for both school.
- Require all users to always log off when they have finished working or are leaving the computer unattended;
- When a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

- Have set-up the network so that users cannot download executable files / programmes without administrator privileges.
- Make clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date.
- Make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Have integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Do not allow personal devices to be connected to our network.
- Have a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements. Hosted via DWM;
- Use the DfE secure s2s website for all CTF files sent to other schools;
- Ensure that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.

Passwords policy

- All teacher laptops / devices that contain key data are encrypted.
- Staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

At Finedon Schools:

- We provide staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work and are provided with approved email accounts. These are monitored for appropriate content and pupils know that they must immediately tell a teacher if they receive offensive e-mail.
- Access in school to external personal e-mail accounts is not allowed

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

School website

- The ICT Junior School Deputy Head takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers – School Administrator. However, the teachers have access to upload information to their class page only.
- The school web site complies with the statutory DfE guidelines for publications;
- Pupil's full names will not be used anywhere on the website, particularly in association with photograph.
- Consent from parents will be obtained before photographs of pupils are published on the school website.

Social networking

Social networking Internet sites (such as, Instagram, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of certain social network spaces, such as Facebook, outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information.
- They maintain professional conduct in and out of the school and do not upload things to social networking sites that could bring themselves or the school into disrepute.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- If a pupil has permission from the Head or Deputy headteacher to bring their phone into school it is handed into the school office at 8:45 and collected at the end of the day.
- Staff should always use school phone to contact parents or where that is not possible ensure that they block their phone number before making the phone call.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Parents cannot use mobile phones on school trips to take pictures of the children.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices:

- All staff are DBS checked and records are held in one central register.

- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form.
  - staff,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.

Technical Solutions

- Staff have a secure area on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- DWM have secure remote access to the server and all laptops in the school in order to deal with any technical issues or security breaches.
- The server is in a lockable cabinet in the loft above the office in the junior school and is managed by DWM technical solutions
- We have off-site back up managed by DWM technical solutions.
- Paper based sensitive information is shredded.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory held by DWM
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency.
- All redundant equipment that may have held personal data will have the storage media wiped. Alternatively, if the storage media has failed, it will be physically destroyed.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendix 1.

Staff Acceptable Use Agreement / Code of conduct in relation to E-saftey: Staff agreement form

ICT and the related technologies such as email, the Internet, IPads and mobile phones are an expected part of our daily working life in school. This agreement 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 agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-Safety Coordinator.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will not reveal my passwords to anyone.
- I will only use the approved, secure email system(s) for any school business.
- I will not allow unauthorised individuals to access email / Internet or any related technologies.
- I will ensure that personal data about children is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will only use the approved school email, teachers 2 parents text system or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without consent of the parent/ carer.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home or on personal laptops.
- 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 the Headteacher.
- 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.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand the policy and my responsibility in remaining professional at all times particularly in reference to social networking sites. I will make sure that privacy settings are activated to protect myself and the school.

- I agree to the points noted regarding social networking and mobile phones on page 10 of the policy.

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

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

Signature ....Date ....

Full Name .... (printed)

Job title ....

School ....

Authorised Signature ICT leader / e-safety co-ordinator

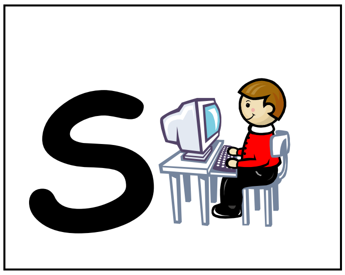
I approve this user to be set-up.

Signature .... Date ....

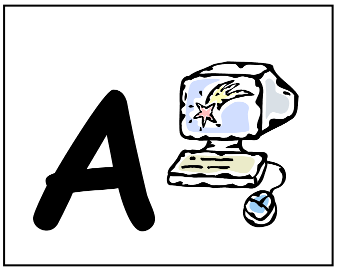
Full Name .... (printed)

Appendix 2 – KS1 pupil agreement.

Think before you click

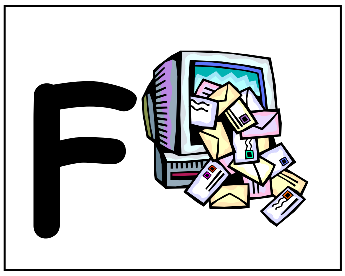


I will only use the Internet, email and computing equipment with an adult's permission and I will use it carefully.

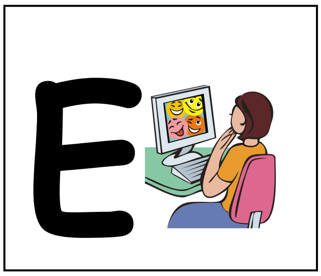


I will keep my login and password information secret.

I will only send friendly and polite messages.



If I see something I don't like or makes me feel unhappy, I will always tell an adult.



I will not send my phone number, address or a photo of me to anybody.

My Name:

My Signature:

Appendix 2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*