Doddiscombsleigh Primary School

E SAFETY POLICY

Rational

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe access to the internet and other communication technologies at all times.

Doddiscombsleigh Primary School must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce any risks. The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors' committee and full governor meetings

Executive Headteacher/Head of School

- The Executive Headteacher is responsible for ensuring the safety (including e-safety) of members of the United Schools Management Partnership community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Executive Headteacher/Head of School is responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Executive Headteacher/Head of School will ensure that there is a system in place to allow for monitoring and support of those in United Schools Management Partnership who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head of School will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Executive Headteacher and Head of School are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The E-Safety Co-ordinator is the Senior IT Technician from the USF.

E-Safety Co-ordinator:

- leads the e-safety committee;
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;

- provides training and advice for staff;
- ensures that staff are regularly reminded of their duty to control the use of personal devices i.e. (1) that they are protected by a PIN/Password/Fingerprint and encrypted where possible, (2) webmail is not left logged in and (3) that attachments are not opened unless in an emergency (as these download to the telephone);
- ensure that staff are regularly reminded to (a) lock screens when unattended, (b) reference the new Data Protection Act 2018 and GDPR, (c) only open attachments or click on links on emails that they were expecting and if they do not look or feel right to check with the sender by other trusted means (e.g. a telephone call or SMS), and (d) to take additional measures to secure special categories of personal data *(data relating to race/ethnicity, religion, genetics, health, photos, sexual orientation, trade union, political opinions*) by ensuring it is locked away when not in use and is kept on their person when transporting it offsite (when it is in unencrypted form e.g. paper)
- liaises with the Local Authority;
- liaises with school ICT technical staff;
- liases with the school's Data Protection Lead and/or the school's Data Protection Officer
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs;
- attends relevant meeting/committee of governors;
- reports regularly to the Head of School.

Senior IT Technician:
ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack (anti-virus software, spyware, user permission to access server, limit on PC settings);
- that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are changed monthly;
- that the use of the network/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator/Executive Headteacher/Head of School/ ICT Co-ordinator for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in Doddiscombsleigh Primary School policies.

Teaching and Support Staff
are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Doddiscombsleigh e-safety policy and practices;
- they have read, understood and signed the Doddiscombsleigh Staff Acceptable Use Policy/Agreement (AUP);
- they report any suspected misuse or problem to the E-Safety Co-ordinator/Executive Headteacher/Head of School/ICT Co-ordinator/Class Teacher (as in the section above) for investigation/action/sanction;
- digital communications with pupils (email/Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- pupils understand and follow the Doddiscombsleigh e-safety and acceptable use policy. Staff are aware of any children who have not, and what this means for their usage of ICT;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations – training to be given on copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are 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 Doddiscombsleigh Primary School policies with regard to these devices;

- in lessons where internet use if pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection/Child Protection Officer:
should be trained in e-safety issues 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.

E-Safety Committee
Members of the E-Safety Committee (or other relevant group) will assist the E-Safety Co-ordinator (or other relevant person, as above) with:

- the production/review/monitoring of the school's E-Safety Policy/documents;
- the production/review/monitoring of the school filtering policy (if the school chooses to have one).

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (note – 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;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand the school's policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying;
- should 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.

Parents/Carers
Doddiscombsleigh Primary School will, therefore, take every opportunity to help parents understand the importance of e-safety through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature.
Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website/on-line pupil/pupil records in accordance with the relevant school Policy.

Community Users
Community Users who access school ICT systems as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

E-Safety Pupils
A planned e-safety programme should be provided as part of ICT/PHSE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**Tutorial/pastoral activities**

- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet will be posted in all rooms and displayed on log-on screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

E-Safety Parents
The United Schools Federation will, therefore, seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website, VLE
- Parents' evenings

E-Safety extended schools
Doddiscombsleigh Primary school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Monitoring
Doddiscombsleigh Primary School will monitor the impact of the policy using:

- Logs of reported incidents.
- DNS Filter and Securly monitoring logs of internet activity (including sites visited).
- Internal monitoring data for network activity.
- Surveys/questionnaires of: pupils, parents/carers and staff.

Education & Training – Staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs for all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Co-ordinator will provide advice/guidance/training as required to individuals as required.

Training – Governors
Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any committee/group involved in ICT/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring
Doddiscombsleigh Primary School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of the school's ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to the school's ICT systems.

- All users will be provided with a group username and password.
- The "administrator" passwords for the school's ICT system, used by the IT Technician (or other person) must also be available to the Executive Headteacher/Head of School and kept in a secure place (e.g. the school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by DNS Filter and Securly.
- Doddiscombsleigh Primary School has provided enhanced user-level filtering through the use of the DNS Filter and Securly.
- In the event of the IT Technician (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by a nominated senior leader.
- Any filtering issues should be reported immediately to DNS Filter.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the Executive Headteacher/IT Co-ordinator (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:

- in lessons where the internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Technician (or other relevant person) can temporarily remove specific sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published.
- Pupils' work can only be published with the permission of the pupil, parent or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2098 and the General Data Protection Regulation which states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
-
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
-
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
-
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
-
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the law in order to safeguard the rights and freedoms of individuals;
-
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Staff must ensure that they:

- at all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data, or lock their screen (using ⊞ +L) when temporarily away from their device;
- transfer data using encryption and secure password protected devices.

When personal data is stored on any school owned and managed portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred back to the school network or its use is complete – which must be done as soon as possible
- When using a personal device (e.g. a device which is not owned and managed by the school):

- The device will be protected by a PIN/Password/Fingerprint and encrypted where possible,
- It will not have school webmail left logged in
- Attachments on personal devices are not opened unless in an emergency (as these download to the un-managed device).
- It will not have any school personal data on the personal device, instead it will be worked on, processed and stored the data on the school network or storage systems (e.g. OneDrive, SharePoint)

This policy will be reviewed annually.

APPENDIX

Staff (and Volunteer) Acceptable Use Policy Agreement (updated Oct 18)

Doddiscombsleigh Primary School Policy
This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that ICT systems and users within the United Schools Federation are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of ICT in their everyday work.

Acceptable Use Policy Agreement
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the parameters agreed by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password (other than the ICT Co-ordinator/Technician).
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to either the ICT technician/ICT Co-ordinator or Head of School.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Doddiscombsleigh Primary School and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by Doddiscombsleigh Primary School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or

may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, without consultation with the ICT Co-ordinator or technician.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

Name …… Signed ……..

Date …….