DHEKELIA PRIMARY SCHOOL

Dhekelia Primary School

e-Safety and Acceptable Use Policy

Reviewed October 2020

E-Safety & Acceptable Use Policy

Schedule for Review

This policy will be reviewed annually to reflect the ever increasing role of technology changes within society.

Scope of the Policy

This policy applies to all members of Dhekelia Primary School and its community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the Dhekelia Primary School.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. **Headteacher and Senior Leaders:**

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of all members of the school community.
- The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents "Responding to incidents of misuse".
- The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school 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 Headteacher and Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.

E-Safety Officer:

It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e-safety, some schools may choose to combine this with the Child Protection / Safeguarding Officer role. At Dhekelia Primary School, Anna Vrahimi (Designated Safeguarding Senior) and Joel Stokoe (Computing Leader) are responsible for any e-Safety incidents. See below for specifics responsibilities

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies. (Joel Stokoe)
- Ensures that all staff are aware of the procedures that need to be followed in the event of an esafety incident taking place. (Anna Vrahimi)
- Provides training and advice for staff. (Joel Stokoe)
- Liaises with school technical staff. (Joel Stokoe)
- Recieves reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Anna Vrahimi)

- Meets regularly with Safeguarding Governor to discuss current issues and review incident logs. (Joel Stokoe/Anna Vrahimi)
- Reports regularly to Senior Leadership Team (Joel Stokoe)

Technical staff:

The Technical Staff is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the hardware and network is regularly monitored in order that any misuse can be reported to the e-safety officer and Headteacher.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the e-safety officer and Headteacher.
- All digital communications with pupils 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 activities.
- Pupils understand and follow the e-safety and acceptable use policies.
- In lessons where internet use is 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.

Child Protection Officer

The child protection officer should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- access to extremist material
- access to illegal and inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- Are responsible for using the school's technology in accordance with the Pupil Acceptable Use Policy.
- Need to understand the importance of reporting anything which they are unhappy with and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good e-safety practice The school will take every opportunity to help parents understand these issues.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.
- A planned e-safety curriculum should be provided as part of Computing lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- 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 Agreements.
- This E-Safety policy and any updates will be presented to and discussed by staff.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The ICT technical services 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 will be effective in carrying out their e-safety responsibilities.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or

downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers 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.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
  It has a Data Protection Policy
- **It has clear and understood arrangements for the security, storage and transfer of personal data**
- **There are clear and understood policies and routines for the deletion and disposal of data**

Staff must ensure that they:

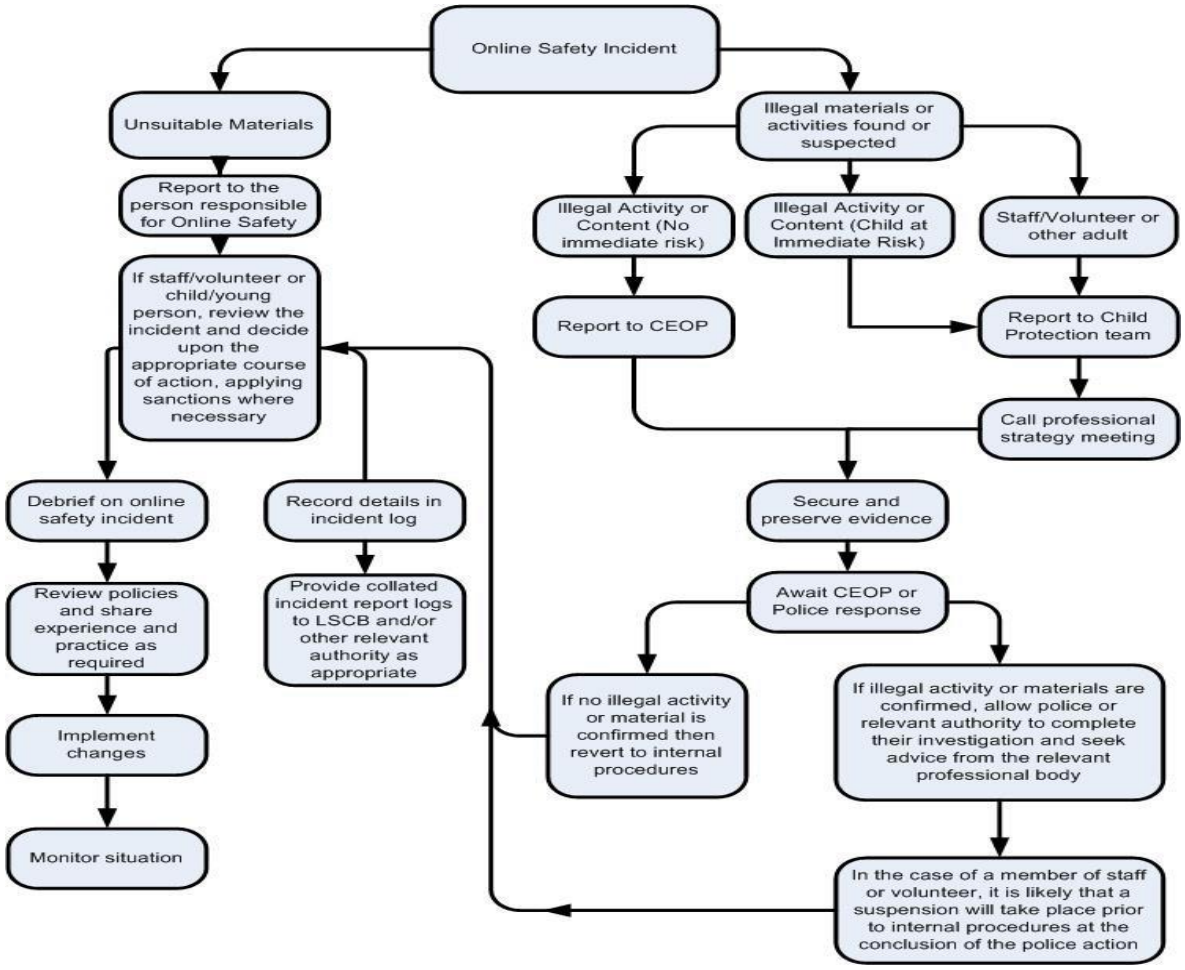
- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**

When personal data is stored on any portable computer system, memory 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 or its use is complete

Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to



online safety incidents and report immediately to the police.

Online safety

In school

We will continue to have appropriate filtering and monitoring systems in place in school.

Outside school

Where staff are interacting with children online, they will continue to follow our existing staff behaviour policy/code of conduct/IT acceptable use policy

Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our reporting procedures as set out in section 3 of this addendum We will make sure children know how to report any concerns they have back to our school, and signpost them to other sources of support too.

Working with parents and carers

We will make sure parents and carers:

Are aware of the potential risks to children online and the importance of staying safe online

Know what our school is asking children to do online, where relevant, including what sites they will be using and who they will be interacting with from our school

Are aware that they should only use reputable online companies or tutors if they wish to supplement the teaching and resources our school provides

Know where else they can go for support to keep their children safe online

This will be presented through the weekly Grapevine, the use of Seesaw and regular emails.