E-Safety Policy

Important information: This policy sits alongside Dovecotes Primary School's Policy Statement for E-Safety (Digital Safeguarding), which can be found on the Dovecotes Primary School website. The Switch Project's ICT infrastructure sits within the School's and is governed by their systems and protocols. As such, we must give regard to and co-operate with their policy. This policy gives information and guidance on the elements specific to The Switch Project's roles and responsibilities but should not be considered in isolation.

ICT Infrastructure

The Switch Project's technical infrastructure is secure and not open to misuse or malicious attack: This status is maintained by Dovecotes Primary School. The school also ensures that it meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply. The hardware is the property of The Switch Project Ltd.

Role and Responsibilities

The Director (or member of staff nominated to deputise):

- is responsible for the approval of the E-Safety Policy and for ensuring that it reflects and supports any relevant changes to the School's Policy.
- has a duty of care for ensuring the safety (including e-safety) of members of The Switch Project community. He may decide to delegate elements of this to other staff where appropriate.
- should be aware of the procedures to be followed in the event of a serious allegation being made against a member of staff.
- is responsible for ensuring that all staff have received suitable training on e-safety. A planned programme of formal E-Safety training will be made available to staff. This will be regularly updated and reinforced. All new staff should receive e-safety training as part of their induction.
- will contact either the school's E-Safety Officer, or a suitably qualified and experienced consultant with any concerns or if there is a need for additional advice.
- will ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed regularly.

- is responsible for the upkeep and maintenance of the hardware and ensuring that the software is up to date and appropriate.

Staff:

- must engage effectively with any training, research or development that they are directed to as well as use their own initiative to maintain an awareness of e-safety matters.
- must demonstrate that they have read, understood and signed this policy and the Staff Acceptable Use Policy/Agreement.
- must report any suspected misuse or problem to The Director immediately.
- must keep all digital communication with students/pupils/parents/carers on a professional level. Any contact with a young person must be reported to The Director.
- should ensure that all attendees of The Switch Project are made aware of what is acceptable and what is not during their induction.
- should, where possible, include E-Safety information in the planning and delivery of activities.
- must monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regards to these devices.
- must not use their own devices in the main room. Staff are free to use their phones etc.. in the office whenever they are able to.
- must only use The Switch Project's equipment to take photos that include the young people.
- must pre-check any websites or digital context that they plan to use prior to the sessions.
- must seek approval from The Director before making reference to Switch on social media or online. No reference should be made to specific young people, parents/carers or school staff without parental (or direct, in the case of adults) permission.
- must not engage in online discussion on personal matters relating to members of the Switch community.
- should not attribute personal opinions to The Switch Project.

Safeguarding (DSL – Tim Wakefield, Director. Deputy DSL – Caroline Erskine-Murphy.)

The DSL and Deputy DSL should have regard to e-safety within a Safeguarding context and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Young People:

- are responsible for following The Switch Project's Student Handbook and the information given to them during their induction. They must have regard to all relevant E-Safety information and requirements given to them whilst using The Switch Project digital technology systems.
- must adhere to the principles of good research and the need to avoid plagiarism and uphold copyright regulations.
- should report any misuse immediately to a member of staff.
- must not use their mobile phones in the main room without specific permission.
- must never take photographs or videos of other young people or staff whilst on the premises. If off the premises then they must obtain the individual's permission before doing so.
- should realise that The Switch Project's policies and their home school's policies could be applied to their actions outside of school or Switch.

Parents

- must have regard to the information about E-Safety within the Parent Handbook

E-Safety Education

- We regularly engage external professionals to run E-Safety workshops as well as cover the topic within many of our sessions. However, due to the often part-time and short-term nature of our provision, it is impossible to guarantee to cover the topic with every Young Person.
- Principal E-Safety messages should be reinforced as part of any planned use of digital technologies.
- Young people should regularly be made aware of the materials/content they access online and be guided to validate the accuracy of information.
- Young people should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in the use of digital technologies/mobile devices/the internet.
- In sessions 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 put in place for dealing with any unsuitable material that is found in internet searches.
- Where young people are allowed to search the internet freely, 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 education reasons, students may need to research topics that may normally result in internet searches being blocked. Staff can request access to those sites via the school's processes. Such requests should be logged with clear reasons.

Training:

All staff are directed to follow the Hayes Education Online Training in Safeguarding and Child Protection, including the Online Safety module.

Digital images:

- 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 and such publishing in school or on school devices is strictly prohibited.
- Staff and volunteers are allowed to take digital/video images that to support educational aims, but must follow Switch policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on Switch equipment; the personal equipment of staff should not be used.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school website.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals/Switch into disrepute.
- Young people must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include young people will be selected carefully and will comply with good practice guidance on the use of such images, including parental consent.
- Young people's full names will not be used on websites/blogs, particularly in association with photographs.
- Young people's work can only be published with the permission of the pupil and parents or carers.

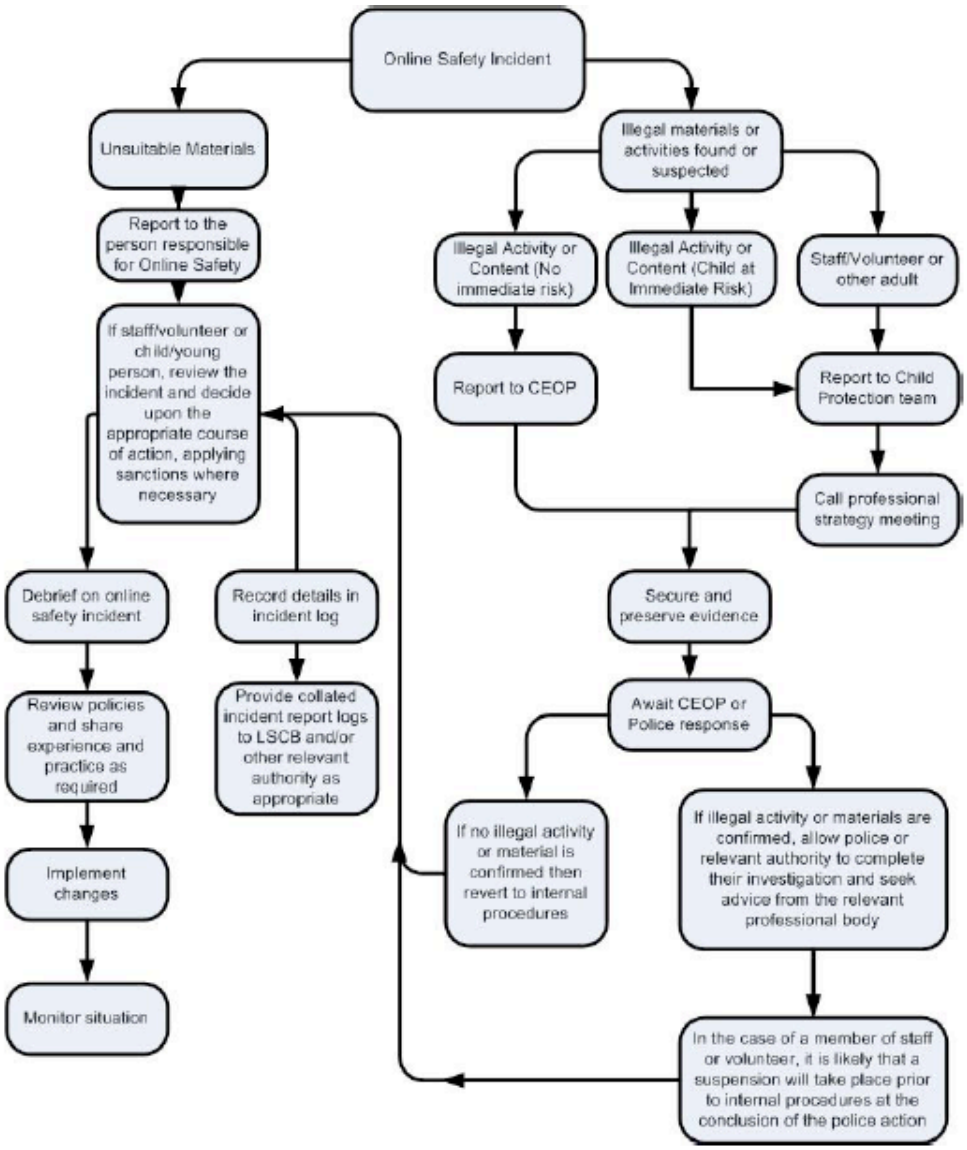
Communications

- The official Switch email service may be regarded as safe and secure.
- Users must immediately report to The Director the receipt of any communication that makes them feel uncomfortable, is offensive/discriminating/threatening/bullying in nature and must not respond to such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official Switch systems. Personal email addresses, text messaging or social media must not be used for these communications unless in an emergency. If this becomes necessary then details must be logged carefully.
- The Switch Project's use of social media will be authorised and monitored by The Director.

Misuse

Illegal 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 for responding to online safety incidents and report immediately to the police.



Other incidents

In the event of suspicion, all steps in this procedure should be followed

- Have more than one senior member of staff/volunteer involved in this process. This vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the

police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have the appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for the investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national/local organisation (as relevant)
  - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of grooming behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation

It is important that all of the above steps are taken as they will provide an evidence trail for the school/academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

We are committed to reviewing our policy and good practice annually.

This policy was last reviewed on: 3rd October 2018