E-SAFETY POLICY

Introduction

The purpose of this document is intended to address the use in the establishment by users (including but not limited to Employee, Students, Visitors, Contractors) of the Internet and specifically E-Safety. This document applies to all users of the Establishment IT System and applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

The establishment recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the establishment while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety guidance should be read alongside other relevant establishment policies; Safeguarding and ICT Acceptable Use Policy.

1. Roles & Responsibilities

The first point of contact should be Central Services. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be staff within establishment.

Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the safeguarding officer may be asked to intervene with appropriate additional support from external agencies.

The Head Teacher is the main contact for safeguarding within the establishment, with deputy Head Teacher and Central Services also able to offer advice and guidance on technical related matters.

Staff

All staff are responsible for using establishment IT systems and mobile devices in accordance with the establishment ICT Acceptable Use Policy and the e-safety Guidance, which they must acknowledge acceptance of.
Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with the establishment ICT Acceptable Use Policy. Online communication with learners is restricted to the establishment network.

External platforms not hosted by the establishment, such as social media sites, may be used following consultation with Central Services This document will, however, be monitored and kept under review.

All staff should apply relevant establishment policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Head Teacher and/or Central services without delay

Learner
Learners are responsible for using the establishment IT systems and mobile devices in accordance with the establishment ICT Acceptable Use Policy and e-Safety Rules, which they must acknowledge acceptance of.

Learners must act safely and responsibly at all times when using the internet and/or mobile technologies.
They are responsible for responding to e-safety information and are expected to know and act in line with other relevant establishment policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the establishment

2. Security

The establishment will do all that it can to make sure the establishment network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of Establishment systems and information. Digital communications, including email and internet postings, over the establishment network, may be monitored in line with the ICT Acceptable Use Policy.

3. Behaviour

The establishment will ensure that all users of technologies adhere to the standard of behaviour as set out in the ICT Acceptable Use Policy.

The establishment will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary expectations.

Where conduct is found to be unacceptable, the establishment will deal with the matter internally. Where conduct is considered illegal, the Establishment will report the matter to the police.

4. Communications

The establishment requires all users of IT to adhere to the establishment ICT Acceptable Usage Policy (which includes Social Media). Any extension of this guidance will require express written permission of a member of SMT.

5. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Advice should be sought by staff where required.

The establishment staff will provide information to learners on the appropriate use of images. This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission.

Photographs of activities on the establishment premises should be considered carefully and have the consent of the student / subject before being published. Approved photographs should not include names of individuals without consent. This is discussed in the establishment Data Protection Policy.

6. Personal Information

Personal information is information about a particular living person. The establishment collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The establishment will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/parent/ carer.

No personal information can be posted to the establishment website unless it is in line with our Data Protection Policy.

For further information see the establishment Data Protection Policy.

All establishment mobile devices such as a laptop, USB (containing personal data) require to be encrypted, password protected and a member of IT Services should be consulted before the data leaves the premises.

However as the establishment operates a highly robust and secure Remote Access system, users should consider using this above all else when working remotely.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy.

7. Information and Training

With the current unlimited nature of internet access, it is impossible for the establishment to eliminate all risks for staff and learners. It is our view therefore, that the establishment should support staff and learners stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners
This guidance will be made available to Learners via staff.

Issues associated with e-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

For staff
Further resources of useful guidance and information will be made available to all staff via Central Services.

Any new or temporary users will receive training on the establishment IT system as part of their induction.

They will also be asked to sign the establishment ICT Acceptable Use Policy.

8. Incidents and Response

Where an e-safety incident is reported to the establishment this matter will be dealt with very seriously. The establishment will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to any tutor or member of staff. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible.

Following any incident, the establishment will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the establishment ICT Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

This policy has been adopted by Churchward School:

Signed …….. Headteacher

Signed …….. Chair of Governors

Date ……