E-safety Policy

Reviewed: September 2020

Next Review Due :01 September 2022

Version Control

Version	Date	Author	Rationale
1	01/11/15		Original
1.1	01/09/18		Reviewed
1.2	01/09/20		Reviewed

Statement

This policy is available for anybody to read on the Academy website; upon review all members of staff will sign as read and understood both the E-safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils' Acceptable Use Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Safeguarding is a serious matter; at Christ Church Academy we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-safety incident, whichever is sooner.

Aim

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

Roles & Responsibilities

1. Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any E-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- The Learning and Teaching Committee will oversee the implementation and review of the policy ensuring they keep up to date with emerging risks and threats through technology use. Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

2. Headteacher/E-safety Officer

Reporting to the governing body, the Headteacher has overall responsibility for E-safety within our school although they may also nominate a specific E-safety officer. The day-to-day management of this will be delegated to all members of staff.

The Headteacher along with the E-safety Officer will ensure that:

- E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- All E-safety incidents are dealt with promptly and appropriately. Staff keep up to date with the latest risks to children whilst using technology; familiarise themself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the staff and governors.
- Staff engage with parents and the school community on E-safety matters at school and/or at home.
- Staff liaise with the local authority, IT technical support and other agencies as required.
- Staff retain responsibility for the E-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Any technical E-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Staff make themselves aware of any reporting function with technical E-safety measures, i.e. internet filtering reporting function; to decide on what reports may be appropriate for viewing.
- All details within this policy are understood by all Staff (teaching and non-teaching).
- If anything is not understood it should be brought to the attention of the Headteacher.
- Any E-safety incident is reported to the headteacher (and an E-safety Incident report is made), or in her absence to the Chair of Governors.
- The reporting flowcharts contained within this E-safety policy are fully understood by all Staff.

3. ICT Technical Support Staff
(Note: Staff bought in for technical support must be given a copy of this policy and sign the front page once read and accepting to agree to the policy as if they are a member of staff)

Technical support staff are responsible for ensuring that:
- The IT technical infrastructure is secure; this will include at a minimum:
  Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any E-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Headteacher.
- Passwords are applied correctly to all users regardless of age and checked termly by Class teachers and Headteacher ensuring change at the end of Key Stage 1.
- The IT System Administrator password is to be changed on a termly basis.

The Technology

Christ Church Academy uses a range of devices including PC's, laptops, Apple I-pads. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use authority recommended filtering software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Headteacher/ICT Coordinator/E-safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are

brought to the attention of the Governing Body. Any additional sites needing to be filtered will be dealt with on an individual basis through the technical support.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and any which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. (Note: Encryption does not mean password protected.)

Passwords – all staff and pupils from Y2 (and Y1 as deemed appropriate by the class teacher) will have an individual password in order to access their personal accounts.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this E-safety and the staff Acceptable Use Policies; pupils upon signing, along with their parents, and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature is not permitted. Similarly use of personal email addresses for work purposes are not permitted.
Pupils are NOT permitted to use the school email system, and will NOT be given their own email address.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Christ Church Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Christ Church Academy and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the E-safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Facebook – used as a closed group closely managed and monitored by the administration team
- Blogging – used by staff and pupils in school (only to be used by those pupils working towards or having completed their SAFE award level 1)
- Twitter – used by the school as a broadcast service (not immediately)
  A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any E-safety incident is to be brought to the immediate attention of the E-safety Officer/Headteacher. The E-safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Christ Church Academy will have an annual programme of training which is suitable to the audience.

E-safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning and posters with reminders will be readily displayed and discussed with children.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-safety Officer/headteacher is responsible for recommending a programme of training and awareness for the school year for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.