Keelby Primary Academy
E Safety Policy 2022

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, academy volunteers, students and any other person working in or on behalf of the academy, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the academy e.g. parent, guardian, carer.

Academy – any academy business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider academy community – students, all staff, governing body, parents, visitors, other schools.

Safeguarding is a serious matter; at Keelby Primary 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.

The primary purpose of this policy is two fold:

- To ensure the requirement to empower the whole academy 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 student or liability to the academy.

This policy is available for visitors on the Keelby Primary Academy website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff and Volunteer Acceptable Use Policy. A copy of this policy and the Pupil Acceptable Use Policy will be sent home with students upon admission to school. This will be discussed with pupils in class. Following discussions around the policy, and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Principal

Reporting to the Academy Improvement Committee (AIC), the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Executive Principal will ensure that:

- E-Safety training throughout the academy is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and AIC, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to **Steve Claybourn**.
The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize themselves with the latest research and available resources for academy and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Executive Principal and AIC on all e-safety matters.
- Engage with parents and the academy community on e-safety matters at school and/or at home.
- Liaise with the Academy Trust, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the Academy Trust and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Principal to decide on what reports may be appropriate for viewing.

ICT Technical Support 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 e-safety officer and Principal.
    - Passwords are applied correctly to all users regardless of age

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Executive Principal.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made using CPoms), or in her absence to the Principal. If you are unsure the matter is to be raised with the e-Safety Officer or the Principal to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this academy are given in the Pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, academy newsletters the academy will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the academy needs have to rules in place to ensure that their child can be properly safeguarded. They must adhere to the school's Parent Social Media policy, and will be made aware of their child's Acceptable Use Policy.

Technology

Keelby Primary Academy uses a range of devices including PC's, laptops and iPads. In order to safeguard the students, and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – this 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 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 Principal.

Passwords – all staff and students will be unable to access any device without a username and password. iPads can be accessed without passwords.

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 Principal if there are any concerns. All USB peripherals such as USB key drives 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 and Volunteer Acceptable Use Policy; students upon signing 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 are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
Students are permitted to use the academy email system, and as such will 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 letter; non-return of the permission slip will not be assumed as acceptance.

Notice and take down policy – should it come to the academy's attention that there is a resource which has been inadvertently uploaded onto the school's website, and the academy 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, or in her absence the Principal. 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 academy 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, Keelby Primary Academy will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum; whenever ICT is used in the academy, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.
We also teach discreet safety during an annual safety week in addition to other safety lessons and instruction.
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 is responsible for recommending a programme of training and awareness for the school year to the Principal and responsible Governor 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 Principal for further CPD.

Incident Management process in the event of an eSafety incident

Action to be taken when the breach is made by a member of staff:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the person who is made aware of this will report this to the designated lead for eSafety/safe guarding (Steve Claybourn)	Member of Staff aware of the incident
The eSafety Co-ordinator will conduct an initial fact finding investigation which will ascertain who was involved, what has occurred. If appropriate the user will be restricted from access to the network	S Claybourn
The eSafety Co-ordinator will classify the incident appropriately (high or low severity) and enter details of the incident onto the member of staff's file	SClaybourn
The Principal/Head of School/line manager will have been informed and should be given the results of the initial fact finding investigation	SClaybourn
If appropriate, discussions will take place between the Trust eSafety team, the technical support team and the eSafety co-ordinator to implement any necessary actions e.g. blocking a website	Trust TSS S Claybourn
The Principal/Head of School/line manager will discuss the concerns with the Trust Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The Principal/Head of School/line manager will also discuss with the Trust if the member of staff needs to be suspended or undertake different duties pending the completion of the enquiries.	A Atkin / T Whiting
The Principal/Head of School/line manager will also discuss the incident with the eSafety lead in the Trust as consideration will need to be given to any further actions required.	A Atkin /T Whiting
The strategy meeting process will be completed following the local Child Protection Appendix 4 Allegations Against Staff Protocol	
The designated lead will complete the agencies incident log and send a copy to the Trust's eSafety team	A Atkin /T whiting

Action to be taken when the breach is made by a young person:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policies, the adult will make a decision whether to deal with it themselves by applying a sanction and logging it in CPoms or report it to the Senior Leadership Team. Guidance on severity and possible sanctions is in appendix 1	Member of Staff aware of the incident
The Senior Leadership Team will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed etc	Senior Leadership Team with support from the Executive Principal
The Senior Leadership Team will classify the incident appropriately (high or low severity) and enter details of the incident into CPoms under Safeguarding and make a decision about appropriate sanctions, with support from the Executive Principal if necessary. They will also inform TSS to enable them to make changes to the computer system	Senior Leadership Team with support from Executive Principal
If necessary, the Principal/Head of School will discuss the concerns with the manager of the local safeguarding team to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the local Safeguarding Team will conduct this investigation as required within the Child Protection Procedures	A Atkin / T whiting