The Kassia Academy
Part of KINGS ACADEMY TRUST

E-SAFETY POLICY

Last reviewed: Sept 2024
Next review due by: Sept 2025

We do things differently.....

H. E. R. E

HIGH STANDARDS EMPATHY RESILIENCE EMOTIONAL RESPONSE

Contents

Purpose

This e-Safety Policy applies to all members of the Kassia community (including staff, learners/learners, volunteers, parents/carers, visitors, community users) who have access to and are users of our ICT systems and mobile technologies, both in and out of Kassia. The purpose of this Policy is to provide the staff appropriate procedures for the protection of safeguarding of children when interacting with information and communication technology. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. Any questions regarding its operation should be addressed to the Head of School, Mr. Karl Hanna.

The Kassia Academy must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating learners and staff about responsible use. Children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can lead to civil, disciplinary and criminal action being taken against staff, learners and members of the wider community. It is crucial that individuals in all settings are aware of the offline consequences that online actions can have. Schools/Academies must be aware of their legal obligations to safeguard and protect children on and offline. The accountability of these decisions will sit with the Head Teacher and the Governing Body.

Designated person for Safeguarding: Mr. Karl Hanna

Deputy Designated person for Safeguarding: Mrs Kirsty Cooper, Mrs Jo Taylor, Mrs Tracy Willcock and Miss Emma Wilcox.

Governor for Safeguarding: Mr. Jacob Bond

Scope of the Policy

This policy applies to all members of The Kassia community (including staff, learners/learners, volunteers, parents/carers, visitors, community users) who have access to and are users of Kassia ICT systems and mobile technologies, both in and out of The Kassia Academy.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within The Kassia Academy:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head of School: Karl Hanna

The Head of School is responsible for ensuring the safety (including e-safety) of members of The Kassia Academy.

The Head of School 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.

Teaching and Support Staff

- They have an up to date awareness of e-safety matters and of the current The Kassia Academy e-safety policy and practices.
- They report any suspected misuse or problem to Mr. Karl Hanna for investigation/action/sanction.
- They use ICT responsibly in lessons
- Promote safe use of ICT and devices

Designated person for child protection/Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious Child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying
- any instances of children enacting or experiencing inappropriate contact, content or conduct, whether by accident or by choice, in a range of settings and contexts

Learners/learners

- Are responsible for using Kassia ICT systems, online communication and collaboration platforms, and mobile technologies in accordance with the Learner Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The Kassia Academy will take every opportunity to help parents understand these issues through parents' evenings, letters and collaboration where appropriate, using these methods to share school-specific information and broader advice from national/ local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Learner/Learner Acceptable Use Policy
- Supporting their child to ICT safely.
- E-Safety Education and Training Education – learners / learners
- Safety education will be provided in the following ways:

A planned e-safety programme will be provided as part of PHSE - this will include, but not be limited to, the safe and appropriate use of ICT systems, online communication and collaboration platforms, and mobile technologies in and outside school.

Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

Learners/learners will be taught in all lessons to be critically aware of the materials/content they access on- line and be guided to validate the accuracy of information.

Why is the use of connected devices important?

At The Kassia Academy, we are aiming to equip our learners with the tools needed to develop both skills for life such as effective information gathering with a view to sources and reliability. We also aim to prepare learners for a job market where administrative and creative uses of computing technology are increasingly considered essential skills.

Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. Kassia has a duty to provide learners with quality Internet access as part of their learning experience.

Learners use the Internet widely outside Kassia and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in Kassia is to raise educational standards, to promote learner achievement, to support the professional work of staff and to enhance The Kassia Academy's management functions.

Internet access is an entitlement for learners who show a responsible and mature approach to its use.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased learner attainment.

- Benefits of using the Internet in education include:
- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools/academies;
- educational and cultural exchanges between learners worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for learners and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of school/academies, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

How will learners learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc. provide an opportunity for learners to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Learners will use age-appropriate tools to research Internet content.
The evaluation of online materials and information exchange methods is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that
- some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand Kassia e-safety policy and Acceptable Use Policies.

Monitoring Security Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and learners.

Local Area Network (LAN) security issues:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For Kassia staff, flouting the Acceptable Use policy is regarded as a reason for disciplinary procedures.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN):

Warrington Borough Council Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools/academies. Decisions on WAN security are made on a partnership between The Kassia Academy and technical service providers

The Kassia Academy will work with Edac Solutions to ensure that:

- Virus protection will be updated regularly.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on Kassia's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access Kassia's network will be enforced.
- Communications are managed
- Electronic communication and collaboration is an essential means of interaction for both staff and learners. Directed use of platforms such as Google Classroom and E-Twinning can bring significant educational benefits; interesting projects between schools/academies in neighboring areas and in different continents can be created, for example.

The implications of the use of communication and collaboration technologies for Kassia and learners need to be thought through and appropriate safety measures put in place. Unregulated access to these platforms can provide routes to learners that bypass the traditional boundaries.

At The Kassia Academy, email and other forms of online communication should not be considered private - most schools/academies and many firms reserve the right to monitor electronic communication using in- house systems. There is a balance to be achieved between necessary monitoring to maintain the safety of learners and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided account to communicate with parents/carers, learners and other professionals for any official academy business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- User names and domains will not be provided which can be used to identify both a learner's full name and the academy. Learner accounts will be approved and managed by The Kassia Academy.
- Learners may only use approved accounts for The Kassia Academy purposes.
- Learners must immediately tell a designated member of staff if they receive offensive electronic communication in any form.
- Learners must not reveal personal details of themselves or others in online communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official The Kassia Academy provided accounts to communicate with learners and parents/carers, as approved by the Senior Leadership Team.
- Access to external personal accounts on communication and collaboration platforms may be blocked.
- Communications sent by staff to external organisations should be written carefully before sending, in the same way as a letter written on The Kassia Academy headed paper would be.
- Communications sent by learners to external organisations should only be done under staff supervision and approved before sending.

How will published content be managed?

Sensitive information about schools/academies and learners could be found in a newsletter but a school/ academy website is more widely available. Publication of any information online should always be considered from a personal and school/academy security viewpoint. Material such as staff lists or a school/academy plan may be better published in The Kassia Academy handbook or on a secure part of the website which requires authentication.

The contact details on the website should be the Kassia address, email and telephone number. Staff or learners' personal information must not be published. Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

The head teacher will take overall editorial responsibility for online content published by The Kassia Academy and will ensure that content published is accurate and appropriate.

The Kassia Academy website will comply with guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing Learners Work

The publishing of learners' names with their images is not acceptable. Published images could be reused, particularly if large images of individual learners are shown.

Strategies include using relatively small images of groups of learners and possibly even using images that do not show faces at all. "Over the shoulder" shots can still convey the educational activity without revealing a learner's identity. Personal photographs can be replaced with drawn self-portraits, images of learners' work or of a team activity. Learners in photographs should, of course, be appropriately clothed photographs of learners performing sporting activities, particularly dance, gymnastics or swimming, should be considered with particular care.

Images of a learner should not be published without the parent's or carer's written permission. Learners also need to be taught the reasons for caution in publishing personal information and images online.

Images or videos that include learners will be selected carefully and will not provide material that could be reused.

Learners' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before images/videos of learners are electronically published.

A list of all learners for whom permission to appear in photographs or videos has not been given, or has been withdrawn, will be kept up to date and made available to all staff. Staff are responsible for ensuring they only use images of learners for whom permission has been given.

Learners' work can only be published with their or their parents /carers' permission.
Written consent will be kept by Kassia where learners' images and work are used for publicity purposes, until the material is no longer in use.

Managing social Media

Parents and teachers need to be aware that the internet has a constantly changing landscape of online spaces and social networks, which allow individuals to publish unmoderated content. Social networks can target content, advertising and invitations to connect with other people based on shared interests, location, age, or any other personal information users choose to share with or on the site/app. Users may be able to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networks provide easy to use, free facilities, although advertising often intrudes and some networks may be dubious in content. Learners should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally (with or without learner involvement or awareness) or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples of social media and personal publishing tools include but are not limited to blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and professional collaboration resources.

Kassia will control access to social media and social networks.

Learners will be advised never to give out personal details of any kind, which may identify them or their location. Examples include but are not limited to real name, address, mobile or landline phone numbers, school/academy attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Staff wishing to use Social Media tools with learners as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

Staff official blogs or wikis should be password protected and run from systems or accounts sourced and managed by Kassia, such as on the approved communication and collaboration platform. Approval should be secured from SLT before material is made publicly accessible. Members of staff are not allowed to run social network spaces for learner use on a personal basis.

Personal publishing will be taught via age appropriate sites that are suitable for educational purposes.

Learners will be advised on security and privacy online and will be encouraged to set strong passwords, deny access to unknown individuals and to block and report unwanted content, contact or conduct they experience online. Learners will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by applying the strongest available privacy settings to their profiles.

All members of The Kassia community are advised not to publish or share specific and detailed private thoughts, especially but not limited to text or images that may be considered threatening, hurtful or defamatory.

Newsgroups, bulletin boards, and forums will be blocked unless a specific use is approved. Concerns regarding learners' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly regarding learners' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of the staff induction process.

Filtering

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day. Warrington I.T Team typically will do this.
- A walled garden or "whitelist" restricts access to a list of approved sites. Such lists inevitably limit
- learners' access to a narrow range of content. This may be deployed therefore for learners who misuse ICT systems but still require internet access for work towards qualifications.
- Dynamic content filtering examines web page content or email for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses.

It is important to note that dynamic content and keyword-based filtering cannot identify and filter content other than text, so this should only be used in conjunction with other access controls.

Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.

Kassia will work with Warrington Bough Council to ensure that filtering policy is continually reviewed.

If staff or learners discover unsuitable sites, the URL will be reported to Kassia SLT who will then record the incident and escalate the concern as appropriate.

The Kassia filtering system will block all sites on the Internet Watch Foundation (IWF) list. Technical staff will consult this list regularly to ensued filtering is up to date.

Changes to Kassia filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

The Kassia Head of School will ensure that regular checks are made to ensure that the filtering methods selected are effective

.

Any material that The Kassia Academy believes is illegal will be reported to appropriate agencies.

User Actions	**Circumstances when allowed**

On-line gaming (educational)	Educational games only, and only when directed and supervised by a staff member
File sharing	File sharing by secure sites only e.g. School accounts on Drop Box, One Drive
Accessing the internet for personal or social use (e.g. online shopping)	Staff only, and only during breaks, before and after school, and not in view of learners
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses	Only with permission of SLT

Good practice guidelines, emails

Best Practise: Staff and learners should only use their school email accounts to communicate with each other.

Safe Practise: Check Kassia's, E-Safety Policy regarding use of your school email or the internet for personal use, e.g. shopping.

Poor Practise: Staff – Do not use your personal email account to communicate with learners and their families without a manager's knowledge or permission and in accordance with this policy. Do not use a school account to send non work related emails.

Images, photos and videos

Best Practise: Only use school equipment for taking pictures and videos. Ensure parental permission is in place. Avoid full face, large scale images wherever possible.

Safe Practise: Check the e-safety policy for any instances where using personal devices may be allowed. Always make sure you have the Head of School/SLT permission before doing so.
Arrange for pictures to be downloaded (and password protected) to The Kassia Academy secure drive, immediately after the event.

Delete images from the devices immediately after downloading.

Poor Practise: Do not download images from organisation equipment to your own equipment. Do not use your own equipment without the Head of School/SLT knowledge or

permission and in accordance with this policy.
Do not retain, copy or distribute images for your own personal use**.**

Internet

Best Practise: Understand how to search safely online and how to report inappropriate content. Make sure there is a valid educational purpose to the use of internet based resources.

Safe Practise: Staff and learners should be aware the monitoring software will log on line activity. Be aware that keystroke monitoring software does just that. This means that if you are online shopping, then your password, credit card numbers and security codes will all be visible to the monitoring technicians.

Poor Practise: Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings. Breach of the E-Safety and Acceptable Use Policy may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile Phones

Best Practise: Staff – If you need to use a mobile phone whilst on school business (trips etc.) The Kassia Academy will provide equipment for you. Make sure you know about inbuilt software/facilities and switch off if appropriate.

Safe Practise: Check the E-Safety Policy for any instances where using personal phones may be allowed. Make sure you know how to employ safety measures like concealing your number by dialing 141 first.

Poor Practise: Do not use your own phone for school purposes with the permission of the Head of School/SLT. Do not retain learner/parental contact details for your personal use.

Social networking (e.g. Facebook/Twitter etc.)

Best Practise: If you have a personal account, regularly check all settings. Ensure you profiles are unsearchable and are not publically accessible, e.g. ‘friends only’. Ask friends and family not to post tagged images of you on their profiles.

Safe Practise: Do not accept people that you do not know as friends Be aware the belonging to a ‘group’ can allow access to your profile.

Poor Practise: Do not have an open access profile that includes inappropriate personal information, statements images, photos or videos.
Do not accept learners or their parents as friends on your personal profile. Do not accept ex learners as friends.
Do not write inappropriate of indiscreet posts about colleagues, learners or their parents etc.

Webcams

Best Practise: Make sure you know about inbuilt software/facilities and disconnect or disable when not in use.

Safe Practise: Check the E-Safety Policy for any instances when using personal devices. Always make sure you have permission from the Head of School/SLT.
Arrange for pictures to be downloaded to the secure Kassia network immediately after the event.
Delete images from the camera/device after downloading.

Poor Practise: Do not download images from organisation equipment to your own equipment. Do not use your own equipment without the Head of School/SLT permission and in accordance with the E-Safety policy.
Do not retain, copy or distribute images for your own personal use.