The Kassia Academy and Support Services (TKAS)
Part of KINGS ACADEMY TRUST

E- SAFETY POLICY

The Kassia Academy and Support Services (TKAS)

Last Reviewed	January 2021
For Review	January 2022

SAFEGUARDING POLICIES CHILDREN AND YOUNG PEOPLE
The safeguarding policies (list back page) are in place to help prevent children and young people up to 18 years of age being at risk of harm. Kassia Academy advises the safeguarding policies are read in conjunction with each other. If you have any concerns or questions regarding policies, please refer to a member of SLT.

WORRIED ABOUT A CHILD/YOUNG PERSON
If you are **worried about a child or a young person** being at risk of harm please speak to DSL Lindsay Regan or DDSL Susan Martin.

EXTREMISM/RADICALISATION
All staff and Governors are to be familiar with the indicators of vulnerability to extremism and radicalisation and the procedures for dealing with concerns. Staff are made aware of the potential indicating factors when a child is vulnerable to being radicalised or exposed to extreme views. These include peer pressure, influence from other people or the internet, bullying, crime and anti-social behaviour, family tensions, race/ hate crime, lack of self-esteem or identity, prejudicial (damaging) behaviour and personal or political grievances. Staff to report any concerns to the **DSL/ DDSL** and record on CPOMS.

SAFEGUARDING /HEALTH AND SAFETY
Kassia Academy is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. At Kassia we provide a caring, positive, safe and stimulating environment that promotes the social, physical and moral development of the individual child and we strive to provide this within our classrooms. All staff follow health and safety guidelines.

SPIRITUAL MORAL SOCIAL & CULTURAL
Kassia aims to prevent children and young people from developing extreme and radical views by embedding SMSC principles throughout the curriculum. During lessons we strive to create a learning environment which promotes respect, diversity and self-awareness and equips all of our children and young people with the knowledge, skills, attitudes and values they will need to succeed in their future lives.

For more details/information on Safeguarding refer to the following documents:

- Keeping Children safe in education (statutory guidance for schools and colleges): July 2018
- Working together to safeguard children (A guide to inter-agency working to safeguard and promote the welfare of children: July 2018
- Guidance for safer working practice for those working with children and young people in educational settings: January 2017
- Safeguarding & Child Protection Procedures (Kassia Academy)

Purpose

This e-Safety Policy applies to all members of the Kassia community (including staff, students/pupils, 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 Mrs. L Regan (Headteacher)

Kassia Academy must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students 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, pupils 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: Mrs. L Regan
Deputy Designated person for Safeguarding: Mrs. S Martin

Governor for Safeguarding: Mr J Leonard

Scope of the Policy

This policy applies to all members of the Kassia community (including staff, students/pupils, 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.

Headteacher: Lindsay Regan

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

are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Kassia
- Academy e-safety policy and practices.
- They have read, understood and signed the Kassia Staff Acceptable Use Policy/Agreement (AUP) and click to confirm as part of the login process every subsequent time they access school systems.
- They report any suspected misuse or problem to Lindsay Regan 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

Students/pupils:

- are responsible for using Kassia ICT systems, online communication and collaboration platforms, and mobile technologies in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to systems and click to confirm as part of the login process every subsequent time they access school systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

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 Student/Pupil Acceptable Use Policy
- supporting their child to ICT safely.

E-Safety Education and Training

Education – students / pupils

S. afety 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, 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
- Students/pupils 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 Kassia Academy we are aiming to equip our pupils 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 pupils 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 students with quality Internet access as part of their learning experience.
- Pupils 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 pupil achievement, to support the professional work of staff and to enhance Kassia Academy's management functions.
- Internet access is an entitlement for students 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 pupil 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 pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils 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 pupils 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 pupils 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.

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

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 Kassia Academy and technical service providers

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.

Managing communication

Electronic communication and collaboration is an essential means of interaction for both staff and pupils. Directed use of platforms such as Google Classroom and E-Twinning can bring significant educational benefits; interesting projects between schools/academies in neighbouring areas and in different continents can be created, for example.

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

At 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 pupils 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, pupils 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 student's full name and the academy. Pupil accounts will be approved and managed by Kassia Academy.

- Pupils may only use approved accounts for Kassia Academy purposes.

- Pupils must immediately tell a designated member of staff if they receive offensive electronic communication in any form.
- Pupils 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 Kassia Academy provided accounts to communicate with pupils 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 Kassia Academy headed paper would be. Communications sent by pupils 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 pupils 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 pupils' 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 Kassia Academy and will ensure that content published is accurate and appropriate.
- Kassia Academy website will comply with guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing Pupils Work

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

Strategies include using relatively small images of groups of pupils 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 pupil's identity. Personal photographs can be replaced with drawn self-portraits, images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed – photographs of pupils performing sporting activities, particularly dance, gymnastics or swimming, should be considered with particular care.

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

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' 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 pupils are electronically published.
- A list of all pupils 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 pupils for whom permission has been given.
- Pupils' work can only be published with their, or their parents'/carers' permission.
- Written consent will be kept by Kassia where pupils' 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. Pupils 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 student 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.
- Pupils 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 students 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 pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes.

- Pupils 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. Pupil 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 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 students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly regarding students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in Kassia Acceptable Use Policy.

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. This typically will be done by Warrington I.T Team.
- A walled garden or "whitelist" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of content. This may be deployed as a consequence for pupils 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 pupils discover unsuitable sites, the URL will be reported to Kassia SLT who will then record the incident and escalate the concern as appropriate.
- 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.
- Kassia Headteacher will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that 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 DropBox, 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 pupils
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 Email

Best practice

r **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

Check Kassia e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

DO NOT

Staff: Do not use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

Do not use a school account to send non-work-related emails to external

Images, photos and videos

Best practice

r **DO**

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

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission.

Make arrangements for pictures to be downloaded to password-protected Kassia Academy systems immediately after the event.

Delete images from the device immediately after downloading.

Poor practice

DO NOT

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use.

Internet

Best practice

r **DO**
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 practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

r **DO**

Staff: If you need to use a mobile phone while on school business (trips etc.), Kassia Academy will provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialing 141 first

Poor practice

DO NOT

Staff: Don’t use your own phone for school purposes without the Headteacher/SLT knowledge or permission.

Don’t retain service student/pupil/ parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

.

Best practice

r **DO**

If you have a personal account, regularly check all settings. Ensure your profiles are unsearchable and are not publicly accessible, e.g. “friends only”.

Ask family and friends to not post tagged images of you on their profiles.

Safe practice

Don’t accept people you don’t know as friends.

Be aware that belonging to a ‘group’ can allow access to your profile.

Poor practice

DO NOT

Don’t have an open access profile that includes inappropriate personal information, statements, images, photos or videos.
Staff:

- Don’t accept students/pupils or their parents as friends on your personal profile.
- Don’t accept ex-students/pupils users as friends.
- Don’t write inappropriate or indiscreet posts about colleagues, students/pupils or their parents.

Webcams

Best practice

r **DO**

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

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to Kassia network immediately after the event.

Delete images from the camera/ device after downloading.

Poor practice

☒DO NOT

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don’t retain, copy or distribute images for your personal use.