Kentmere Academy and Nursery

Internet Safety Policy

Kentmere Avenue Rochdale OL12 9EE
Tel: 01706 647533 Web: www.kentmereacademy.co.uk
Email: info@kentmereacademy.co.uk
A partner of the Watergrove Trust.

Regulations (GDPR).

1. INTRODUCTION AND OVERVIEW

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Kentmere Academy with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff of Kentmere Academy
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Extremism exposure.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Sexual abuse. This can take place online, and technology can be used to facilitate offline abuse (Keeping Children Safe in Education, 2020).
- Sexual Harassment. Including non-consensual sharing of sexual images and videos, sexualised online bullying, unwanted sexual comments and messages, including on social media; sexual exploitation; coercion and threats and upskirting (KCSIE, 2020).
- Cyber-bullying in all forms. This can take place wholly online, or technology may be used to facilitate offline abuse (Keeping Children Safe in Education, 2020).
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

- CSE (Child Sexual Exploitation) and CCE (Child Criminal Exploitation)

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Mental Health and well-being (amount of time spent online Internet, impact of cyberbullying or gaming).
- Sexting (sending and receiving of personal intimate content / images).

2. SCOPE

This policy applies to all members of Kentmere Academy community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy.

The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be stored on network location.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The Academy nor the Trust can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by Safe Guarding Officers / Senior Leaders / Headteacher
- Informing parents or carers
- Temporary removal of Internet or computer access for a period
- Referral to LA / Police or other authorities.

Any complaint about staff and student misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

Review and Monitoring

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors.
- The policy is also closely monitored by the Kentmere Academy's Internet Safety Team and any changes required from these meetings are made with consensus with the Headteacher and Governing Body.

3. EDUCATION AND CURRICULUM

Pupil e-safety curriculum

The Academy has a clear, progressive e-safety education programme as part of both the pastoral system and curriculum. It covers a range of skills and behaviours including:

- To STOP and THINK before you CLICK
- To follow the SMART rules for staying safe online
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.

- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To understand how peer on peer abuse can take place online, including sexual harassment (KCSIE, 2020).
- To recognise the impact of technology on mental health and wellbeing.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every pupils will sign and will be displayed throughout the school.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and Governor training

The Academy will:

- Provide, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

- All staff have general safeguarding training yearly which covers elements of e-safety and INSET provided to all staff centred around E-safety is completed.
- Members of the Internet Safety Team have the opportunity to experience training supplied through outside agencies such as the NSPCC. This knowledge and expertise is disseminated through INSET to all staff.

Parent awareness and training

The Academy will:

- Run a rolling programme of advice, guidance and training for parents, including:
- Introduce the Acceptable Use Agreements to new parents, to ensure that principles of e-safety behaviour are made clear.
- Use information leaflets, Internet Safety Day, school newsletters, and the school web site to raise awareness of e-safety.
- Provide suggestions for safe Internet use at home.
- Provide information about national support sites for parents.

4. EXPECTED CONDUCT AND KEY RESPONSIBILITIES

In this school, all users:

- Are responsible for using the school IT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Roles and Responsibilities:

Role	Key Responsibilities

Headteacher	● To take overall responsibility for e-safety provision. ● To ensure the school uses a, filtered Internet Service, which complies with current statutory requirements. ● To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. ● To be aware of procedures to be followed in the event of a serious e-safety incident. ● To receive regular monitoring reports from the E-Safety Co-ordinator / Officer. ● To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. IT manager).
Designated Child Protection Lead & E-Safety Co-ordinator	● Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. ● Promotes an awareness and commitment to e-safeguarding throughout the school community. ● Ensures that e-safety education is embedded across the curriculum. ● Liaises with school ICT technical staff.
	● To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs. ● To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. ● To ensure that an e-safety incident log is kept up to date. ● Facilitates training and advice for all staff. ● Liaises with the Local Authority and relevant agencies. ● Is regularly updated in e-safety issues and legislation, 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 and use of social media

Governors / E-safety governor	● To ensure that the school follows all current e-safety advice to keep the children and staff safe ● To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor ● To support the school in encouraging parents and the wider community to become engaged in e-safety activities ● The role of the E-Safety Governor will include: - regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	● To liaise with the e-safety coordinator regularly ● To oversee the delivery of the e-safety element of the Computing curriculum
IT Manager	● To report any e-safety related issues that arises, to the e-safety coordinator. ● The school's policy on web filtering is applied and updated on a regular basis ● That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant ● That remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction the use of the network.
Teachers	● To embed e-safety issues in all aspects of the curriculum and other school activities ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff	● To read, understand and help promote the school's e-safety policies and guidance ● To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy ● To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices ● To report any suspected misuse or problem to the e-safety coordinator ● To maintain an awareness of current e-safety issues and guidance e.g. through CPD ● To model safe, responsible and professional behaviours in their own use of technology ● To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	● Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. ● To know and understand school policy on the taking / use of images and on cyber-bullying. ● To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school ● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home ● To help the school in the creation/ review of e-safety policies.
Pastoral support	● Educating Parents and raising awareness as instructed by Head / CP designated officer.

Parents/carers	● Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school ● To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. ● To read, understand and promote the school Pupil Acceptable Use Agreement with their children ● To access the school website in accordance with the relevant school Acceptable Use Agreement. ● To consult with the school if they have any concerns about their children's use of technology
External groups	● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

5. MANAGING THE INFRASTRUCTURE

Internet access, security (virus protection) and filtering

The Academy:

- Has an educational filtered secure broadband connectivity provided by the academy trust.
- Uses the academies filtering system which blocks sites that fall into unsuitable categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Blocks all Chat rooms and social networking sites except those that are part of an approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable / useful.
- Works in partnership with the Academy Trust to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of Learning Platforms as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search .

- Never allows / Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search.
- Informs all users that all computer use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator - Wardle helpdesk / teacher / person responsible for URL filtering].
- Makes clear all users know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc.

available for pupils, staff and parents.

- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management

The Academy:

- Ensures IT Staff are up-to-date services and policies.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. [Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to re-enter the network. Any flaws in this must be reported.
  - Has set-up the network so that users cannot download executable files / programmes.
  - Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
  - Makes clear that staff accessing LA systems do so in accordance with any corporate policies. e.g. email or Intranet; finance system, Personnel system etc.
  - Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to the Website Manager and their support team.
- The school website complies with the statutory DfE guidelines for publications and reviewed on a regular basis by the Academy Trust.
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status;

- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geo data in respect of stored images

Social networking

- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the Academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing This school

- Only uses the academy supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained for 30 days*), without permission except where disclosed to the Police as part of a criminal investigation.

6.EQUIPMENT AND DIGITAL CONTENT

Personal mobile phones and mobile devices

Staff, Parents and Visitors.

- Mobile phones and personal handheld devices brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

- No images, videos or recordings should be taken on mobile phones or personally owned handheld devices within the school or its grounds without the prior consent of the Headteacher **and** the person or people concerned.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Staff may use their phones when not supervising children eg. during break times as long as no children are present. If a staff member is expecting a personal call with no pupils present. Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities the only calls to be made are with the school office or emergency services.
- Staff are permitted to connect personal devices to the academies wireless BYOD (Bring Your Own Device) network. All devices connected to this network are logged and filtered under the staff members account. Students
- Students **must not** bring mobile phones or hand held devices into school. If a child is found with a mobile phone, this will be confiscated by the Headteacher/SLT and held in a safe, secure place. Mobile phones and devices will be released to parents or carers at the end of the school day.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Students should protect their personal phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Signed: Sarah Isberg Sarah Isberg (headteacher)

Agreed by the Governing Body:

Date: September 2020

Review: July 2021