FRIARS MULTI ACADEMY TRUST

E-SAFETY

ACCEPTABLE USE POLICY

NON STATUTORY POLICY
Reviewed: April 2021
Approved by Trust Board: 11 May 2021
Next review date by Trust Board: May 2023
Policy Created by: E-safety Leader

Glossary

The term **'School'** is used as standard to mean the educational establishment that is adopting this policy.

The term '**Head teacher'** is used to refer to the person with overall day-to-day responsibility of the **School.**

Directors are the Trustees of the Board.

LGB is the Local Governing Body.

Trust Policy Aims

The term e-Safety is used to encompass the safe use of all online technologies in order to protect children and young people from risks.

This Policy covers the acceptable, safe and responsible use of all online technologies (including internet, apps, email, web cams, instant messaging and other social networking spaces, mobile phones and games). It aims to safeguard adults and children within the school setting and beyond the school environment.

As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children are protected from potential harm both within and beyond the school environment.

It also explains procedures for any unacceptable or misuse of these technologies by adults or children.

The risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile phone device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

Roles and Responsibilities Specific for the Governors and Headteacher of Friars Academy:
It is the overall responsibility of the head teacher along with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the Trust with further responsibilities as follows:

- The Head teacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- A disclaimer should appear on all e-mails from the Academy e-mail address stating the views expressed are not necessarily those of the Academy. The Head teacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Head teacher should inform Governors about the progress or updates to the e-Safety curriculum and ensure Governors know how this relates to child protection.
- The Governors must ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed. It is the responsibility of the Governors to ensure that all Child Protection guidance and practices are embedded.

- An e-Safety Governor (can be ICT or child Protection Governor) will challenge the Academy about having an AUP and especially about: Firewalls, anti-virus software, filters, using an accredited ISP, awareness of wireless technology issues, a clear policy on using personal devices.
- Ensure that any misuse or incident is dealt with appropriately according to policy and procedures.

E-Safety Leader

It is the role of the designated e-Safety Leader to:

- Ensure AUP is reviewed annually, taking into account new and emerging issues and technologies
- Update staff regularly
- Ensure filtering is set to correct level (or inform technician)
- Ensure all adults are aware of filtering levels and why they are there
- Monitor use of the internet and online technologies
- Personal devices should not be used in the Academy.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to section 12 of the Allegation Procedure from the LSCBN to ensure correct procedures are used with incidents of misuse.
- Work alongside the IT Technician regarding antivirus software and the deployment of regular updates.

Staff

It is the responsibility of staff

- To ensure they know who the Designated Person for Child Protection is.
- Be familiar with Behaviour and other relevant policies.
- Alert the e-Safety leader of any new or arising issues that may need to be included in policies and procedures.
- Ensure children are protected and supported in their use of on-line technologies so that children know how to use them in a safe and responsible manner.
- Sign an Acceptable Use Statement when joining the Trust.
- Remember confidentiality.
- Report accidental access to inappropriate materials to the e-Safety Leader and Friars Academy helpdesk so that inappropriate sites can be added to the restricted list.
- Update their anti-virus software regularly on laptops.

Children/Students

Children/Students are

- Involved in the review of our Acceptable Use Rules through the School Council.
- Responsible for following the Acceptable Use Rules whilst within the Academy.
- Taught to use the internet in a safe and responsible manner through ICT and PSHE lessons.
- Taught to tell an adult about any inappropriate materials, without reprimand.
- Taught about the dangers involved with online sites and what to do in the event of witnessing inappropriate use or feeling unsafe.

Appropriate Use by Staff

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which will be signed and returned to your place of work.

The acceptable use should be similar for staff to that of the children/students so that an example of good practice can be established.

In the event of Inappropriate Use

If a member of staff is believed to misuse the internet or any on-line technologies (including social networking sites) in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the

Allegations Procedure (Section 12, LSCBN) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate Use by Children/Students
The rules are there for children/students to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions, e.g. knowing what is polite to write in an e-mail to another child/student or understanding what action to take should there be the rare occurrence of sighting unsuitable materials.

The rules are displayed in each classroom and in the computer suite. All students are asked to sign an acceptance of the rules when joining the Academy.

Parents/carers are also asked to sign an acceptance of the rules to show their support. This is also intended to provide support and information to parents/carers when children/students may be using the internet beyond school. Parents/carers should feel able to add/amend/discuss the rules at any time to reflect any potential issues, as appropriate.

The rules are printed in the school planners when possible, If planners are not available, they are shared with parents via email.

In the Event of Inappropriate Use by Children/Students
- In the event of misuse of the internet access may be taken away for a limited time.
- Additional disciplinary action may be taken in line with existing practice on inappropriate language or behaviour.
- If a student accidentally accesses inappropriate materials the child will report this to an adult immediately.

The Curriculum and Tools for Learning
Students are taught to use the internet and online technologies in a safe and responsible manner within their ICT lessons, PSHE lessons and reinforcement within the classroom.

Personal safety – students are made aware that they should not disclose any personal information on websites or in email, including name, address, telephone number, email address, school, clubs attended and where, age DOB or passwords. Staff, parents and carers should monitor the content of photographs uploaded.

E-mail use
We have email addresses for students to use as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms. Staff and students are to use their official Academy issued email addresses for any communication between home and school only. Parents/carers are encouraged to be involved in the monitoring of emails sent.

Video Conferencing
Web cams/iPads can be made available for video conferencing if felt appropriate. When using this facility in the Academy it will be done under supervision of at least two responsible staff members. Children/students need to ask permission from a member of staff or adult to use this facility both in and beyond school. Children/students need to tell an adult immediately of any inappropriate use by another child/student or adult. (This is part of the Acceptable Use Rules.) Taking images via a web cam will follow the same procedures as taking images with a digital or video camera.

Virtual Lessons
When virtual video calls are required to take place due to pupils learning offsite or staff working offsite, there will always be more than one adult present. Staff and pupils will be appropriately dressed and no

recording of the videos will take place. Students will be provided with a clear list of rules to follow and parents will provide written consent via email to allow their child to take part.

Virtual Learning Video Rules
These rules are also available in the school planners.

1. If you plan on participating with the video, you should take part from a communal area of your home. You should not take part in the video call from your bedroom.
2. Do not use your full name for your user name. Use your first name and initial of your surname. E.g. James B.
3. You should make sure an adult at home knows you are on a video call (adults do not have to join in).
4. You should never record or take photos of your screen during a video call.
5. You should not share the video invite link with anyone that is not in our class.
6. You should dress appropriately for the video call (no pyjamas please).
7. You should respect our normal classroom rules on the call, which means no rude language or inappropriate behaviour.

Mobile phones and other Technologies
The use of mobile phones is not allowed in the Academy. The Academy accept no responsibility for mobile phones brought into the establishment.

Under no circumstances should staff members use their personal numbers to contact students of any age. If contact is to be made in an emergency situation the academy mobile telephones must be used in the presence of another member of staff. Any breach of this procedure will be treated as misconduct and dealt with through the Trust's disciplinary process.

It is also the Trust's policy to ensure that we educate our children/students in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

Video and Photographs
The term image refers to the taking of video footage or photographs via any digital camera or video camera. When in school there is access to digital cameras, video cameras and school laptops. Staff should not use their own personal equipment to take images of children/students in school. Images should only be downloaded onto the school network – If it is necessary to download images onto laptops they should be removed to the school network as soon as possible (or stored onto CD by the ICT Department).

The sharing of photographs online will only occur after permission has been given by a parent/carer or member of staff. Any photographs uploaded should not have a file name of a student, especially where uploaded to a school website. Photographs should only ever include a student's first name. Group photographs are preferable and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.

Filtering and Safeguarding Measures
The Academy utilises a Prevent compliant filtering policy and integrates the Home Office Terrorism Watch List (CTIRU - Counter Terrorism Internet Referral Unit) so that all sites and searches on that list are blocked and cannot be accessed. A banned word list is maintained that is copied from the Internet Watch Foundation, providing us with a baseline of terms that should be filtered and blocked. This list of banned words conforms to terms identified by the DfE as used in ISIL dialogue so that students are unable to use these words to search for related material. Social media sites such as YouTube, Twitter and Facebook are filtered by the academy but can be opened up if necessary to offer flexibility within lessons.

Anti-virus software and Anti malware software is used on all network and laptop PCs and is updated on a regular basis.

A firewall ensures information about our children and the Academy cannot be accessed by unauthorised users.

Children use a search engine that is age appropriate (Bing, Google).

Links or feeds to e-safety websites are provided.

The Headteacher has signed a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirement.

CEOP (Child Exploitation On-line Programme) training for secondary students is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible.

Monitoring
The online safety leader will monitor the use within lessons and extra-curricular activities. A senior member of staff should be monitoring the use of the internet by students and staff, on a regular basis.

Teachers monitor the use of the internet during lessons.

School library & Other online devices
The computers in the library, the iPads, tablets & chrome books, are protected in line with the Academy network. Students should be supervised when using these computers in the same way they would be for curricular lessons using on-line technologies.

Parents

- **Roles** – (There is no statutory requirement for parents to sign acceptable use policies.) Each student will receive a copy of the Acceptable Use Policy on entry to Friars Academy which will be explained in school and should be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules. The Academy will keep a record of the signed forms.

- **Support** – We believe in promoting a positive attitude to using the World Wide Web and therefore want our parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly. We offer all parents the opportunity to find out more about how they can support our school in keeping their child safe whilst using on-line technologies beyond school. Information is regularly posted in our termly newsletter to parents and they can call or visit the Academy at any time for information.

Links to Other Policies

- **Behaviour and Anti-Bullying Policies**
  Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via online communication.
- **Allegation Procedures and the Child Protection Policy**
  Please refer to the Allegation Procedure, section 12, in order to deal with any incidents that occur as a result of using personal mobile or email technologies which may result in an allegation or misuse or misconduct being made by any member of staff.

Allegations should be made to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

The (DFES) DCFS White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people about homework or any other school issues either in or beyond school and any such action should be dealt with. We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

Please refer to the Child Protection Policy for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

- **PSHE**
  We link the teaching and learning of eSafety with our PSHE curriculum by ensuring that the key safety messages are the same whether children are on or off line engaging with other people.
- **Health & Safety**
  Refer to the Health & Safety Policy for information on the safe use of offline technologies. (Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.)
- **Academy Website**
  The uploading of images to the Academy website will be subject to the rules as stated in the Acceptable Use Policy. Permission is always sought from the parent/carer prior to the uploading of any images.

Staff Procedures for Misuse

These procedures should be followed in the event of any misuse of the internet:

a. **An inappropriate website is accessed inadvertently**:
Report website to the e-Safety Leader if this is deemed necessary. Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list. Check the filter level is at the appropriate level for staff use in school.

b. **An inappropriate website is accessed deliberately**:
Ensure that no one else can access the material by shutting down. Log the incident. Report to the Headteacher/e-Safety Leader immediately. Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline. Inform the RA/RBC filtering services as above.

c. **An adult receives inappropriate material**.
Do not forward this material to anyone else – doing so could be an illegal activity. Alert the Headteacher immediately. Ensure the device is removed and log the nature of the material. Contact relevant authorities for further advice e.g. police.

d. **An adult has used ICT equipment inappropriately**:
Follow the procedures for b.

e. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary. Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions. If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy. Contact CEOP (police) as necessary.

f. **Threatening or malicious comments are posted to the academy website (or printed out) about an adult in the Academy**:
Preserve any evidence. Inform the Head teacher immediately and follow Child Protection Policy as necessary. Inform the e-Safety Leader so that new risks can be identified. Contact the police or CEOP as necessary.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance. All staff should know who the Designated Person for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Friars Academy - Acceptable use Rules for Staff

These rules apply to all online use and to anything that may be downloaded or printed.

To ensure that all adults within the academy setting are aware of their responsibilities when using any online technologies, such as the internet or e-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to students for the safe and responsible use of online technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the academy equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to students before they can upload images (video or photographs) to the internet or send them via e-mail.
- I know that images should not be inappropriate or reveal any personal information of children if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that arise, effectively.
- I will report any incidents of concern for student's safety to the Head teacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who the Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail and should use the academy e-mail and phones (if provided) and only to a student's academy e-mail address upon agreed use within the academy.
- I know that I should not be using the academy system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should not use memory sticks or storage devices at school or on academy devices.
- I will not open any attachments or click on a link that appears in an email from an unknown source.
- If I receive a concerning email from an unknown source I will report it immediately to the IT Technician and Headteacher/online safety leader.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the GDP regulations and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-Safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

Friars Academy – e-Safety
Acceptable Use Policy

I have read, understood and agree with these Rules and the guidance for staff use as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard students when using online technologies.

Signed …….. Date ……..

Name (printed) ……..

Student's Procedures for Misuse

These procedures should be followed in the event of any misuse of the internet:

An inappropriate website is accessed inadvertently:

- Reassure the student that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list.
- Check the filter level is at the appropriate level for use in school.

An inappropriate website is accessed deliberately:

- Refer the student to the acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform LA/RBC as above.

An adult or student has communicated with a student or used ICT equipment inappropriately:

- Ensure the student is reassured and remove them from the situation immediately.
- Report to the Headteacher and Designated Person for Child Protection immediately.
- Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
- Contact CEOP (police) as necessary.

Threatening or malicious comments are posted to the academy website about a student in the Academy

- Preserve any evidence.
- Inform the Headteacher immediately.
- Inform the RBC/LA and e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

Dear Parent/Carer

We have recently updated our e-Safety Policy to reflect the use of all online technologies (not just the internet and email). Digital camera and video are being used increasingly and it is vital that students understand how to use them safely.

In order to support the school in educating your child about e-Safety (the safe use of the internet), please read the following e-Safety Rules with your child, then sign and return the form attached. In the event of a breach of the Rules by any child, the e-Safety Policy details further actions and consequences should you wish to view it. The Rules and consequences of any breach have been discussed in school with your child.

These Rules provide an opportunity for further conversation between you and your child about safe and appropriate use of the internet and other online tools (e.g. mobile phone), both at school and outside of school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact the Head Teacher.

Yours faithfully,

Mrs S Ijewsky
Headteacher

e-Safety Acceptable Use Rules Return Slip

Student Agreement:

Name of student: _____ Class _____

- With an adult, I have read and understood the Rules for using the internet, e-mail and online tools, safely and responsibly.
- I know that adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Student Signature _____ Date _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision of children when using the internet, e-mail and online tools. I understand that occasionally inappropriate materials may be accessed and accept that the school will endeavour to ensure this is infrequent and will deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the internet, e-mail and any other facilities outside of school, that it is my responsibility to ensure safe and responsible use.

Parent/Carer signature _____ Date _____

Please return this form to the class teacher.

Our e-Safety Rules

- We will ask permission from an adult before using the Internet.
- We will not break copyright laws.
- We will not use personal storage devices on any computer in school without permission.
- We will use the internet to help us learn and we will learn how to use the internet.
- We will send e-mails and messages that are polite and friendly.
- We will only e-mail or video-conference people an adult has approved.
- Adults are aware when we use online tools, such as video-conferencing.
- We will never give out passwords or personal information (like our surname, address or phone number), without permission.
- We will never post photographs without permission and never include names with photographs.
- We will not access other people's files.
- If we need help we know who to ask.
- If we see anything on the internet or in an e-mail that makes us uncomfortable, we know what to do.
- If we receive a message sent by someone we don't know we know what to do.
- We understand that the internet sites we visit will be monitored.
- We know we should follow the rules as part of the agreement with our parent/carer and know what will happen if we do not.

Further guidance for parents/carers

The following websites offer further information and guidance:

- www.ceop.police.uk
- www.netsmartzkids.org (5-17)
- www.thinkuknow.co.uk
- www.phonebrain.org.uk