GENESIS
EDUCATION TRUST

AUP review Date: Summer 2019

Date of next Review: Summer 2022

Reviewed by: Carlene Reid

Acceptable Use Agreement: All Staff, Volunteers and Governors

This Acceptable Use Agreement covers use of all digital technologies in school: i.e. email, Internet, network resources, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head of School and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / network, or other school systems I have access to.
- I will ensure all documents, data etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will follow the guidance as stipulated through the General Data Protection Regulations (GDPR) and report any Data breaches within 72hours to the Chief Operations officer and the Data Protection Officer.
- I will not access school systems in any public places where data could be seen or on any shared devices which are not password protected.
- I will not view others screens whilst they work in case of viewing personal data.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system for any school business.
  This is currently: GMAIL
- I will only use the approved email system (Gmail), and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact.

- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author’s permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any ‘loaned’ equipment up-to-date, using the school’s recommended anti-virus and other ICT ‘defence’ systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will follow the school’s policy on use of mobile phones / devices at school
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert St Mary’s/ St Saviour’s/ St Margaret’s child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any IT usage (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Head / a senior member of staff / Safeguarding Lead at the school.
- I understand that the levels of filtering in place by Gmail are set to ensure that children are safe from inappropriate, terrorist and extremist material when accessing the Internet at school, and will alert senior members of staff and the child protection officer if I feel any child may be exposed to such material intentionally or otherwise.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

- *Staff that have a teaching role only*: I will embed the school's e-safety / digital literacy curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a ‘safe and responsible digital technologies user’.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .... Date ....

Full Name .... (printed)

Job title / Role ....

Authorised Signature (Executive Principal/Headteacher/ Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature .... Date ....

Full Name .... (printed)

One copy to be retained by member of staff | Second copy for school file

Version: June 2019

The Genesis Education Trust E-safety guidance

What do I do if ….

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head of school /e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered

An inappropriate website is accessed intentionally by a child

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the head of school/ e-safety officer
4. Inform the school technicians and ensure the site is filtered if need be.

An inappropriate website is accessed intentionally by a staff member.

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. In an extreme case where the material is of an illegal nature:
   a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head of school and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head of school should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (undertaken by Headteacher).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head of school and e-safety officer.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

In this instance, we may consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content. You may want to use standard letter template for this which is available from the e-safety leader/ school office.
3. If the game is played within school environment, ensure that the technical team block access to the game

4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are concerned that a child’s safety is at risk because you suspect they have been exposed to terrorist or extremist material online.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child
3. Inform the head of school/ e-safety officer/ child protection officer.
4. Inform the school technicians and ensure the site is filtered if need be.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Headteacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.