www.emmausfederation.co.uk

Safeguarding: E-Safety Policy

Scope of the Policy

The Executive Headteacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity.

As such, this policy is an integral part of our Safeguarding provision. This policy applies to all members of the Emmaus Federation (including staff, pupils, volunteers and visitors) who have access to and are users of school ICT systems, both in and out of the school.

The School fully appreciates the fundamental relationship between E Safety and Pupil Safeguarding and its legal obligations to safeguard all its pupils (See "Safeguarding Policy" and "Keeping Children Safe in Education" DfE, September 2016). The School also recognises that the *Education and Inspections Act 2006* empowers Headteachers to regulate reasonably the behaviour of pupils when they are away from the school site. This is especially pertinent to incidents of cyberbullying, or other E-Safety incidents, which may occur away from the school premises, but are linked to membership of the school. The *2011 Education Act* gave greater powers to Headteachers with regard to the searching of electronic devices and the deletion of data. The School also understands its legal responsibilities under the *Counter-Terrorism and Security Act 2015*, to take every effort to prevent individuals from being drawn into terrorism through the internet or by other means, and to challenge extremist ideas propagated by terrorist organisations.

The School will deal with E-Safety incidents with regard to this policy and other relevant policies (Good Behaviour Policy and Anti-bullying Policy) and seek to keep parents and guardians fully informed of any E-Safety incidents or threats.

Roles and Responsibilities

E-Safety Co-ordinator

From September 2017, the school's E-Safety Co-ordinators are Mrs Hutchinson and Mrs Gray (Head of Schools).

The Governing Body

The Governing Body is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher

The Headteacher, Mrs Collett, has a duty of care for ensuring the safety (including e-safety) of all members of the school community, though the day to day

responsibility for e-safety is delegated to the E-Safety Co-ordinator.

E Safety Co-ordinator (Mrs Hutchinson and Mrs Gray)

- takes responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety documents
- liaises with external authorities and consultancies where necessary
- liaises with school technical staff to ensure network security
- liaises with the Designated Safeguarding Lead to review reports of E-Safety incidents

ICT Coordinator (Mr Grove and Miss Ablard)

- monitoring of the delivery of E-Safety to pupils and wider school community
- e-safety components are assessed at the end of each term
- that the school's technical infrastructure is secure on a day to day basis
- that they keep up to date with e-safety technical information and brief key staff accordingly

Designated Safeguarding Lead (Mrs Hutchinson and Mrs Gray)

- is trained in e-safety issues and aware of the potential for serious child protection and/or safeguarding issues to arise from:
- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Teaching and Support Staff are responsible for ensuring that:

- they have read the E-Safety Policy, Keeping Children Safe in
- Education and signed read the Staff Handbook
- they report any suspected misuse or problems to the E-Safety
- Coordinator
- digital communications with all members of the Emmaus Federation community (pupils, parents, colleagues) must always be conducted on a professional level and **only carried out using official school systems – e.g. Emmaus Fed Twitter site**
- they monitor the use of digital technologies (mobile devices, cameras etc) in lessons and other school activities and implement current policies with regard to these devices.
- Internet use in lessons is pre-planned and closely monitored to ensure pupils do not gain access to inappropriate material (possibly pornography or websites depicting violence or promoting extremist political views)

Pupils:

- are responsible for using the school's ICT systems in accordance with the
- must report any instance of abuse, misuse or access to inappropriate materials to a member of staff
- must know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber- bullying.
- must 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.

Parents & Guardians

Parents play an important role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. This is reflected in the School's Home/School Agreement.

The School will take every opportunity to help parents understand these issues through parents' E- Safety evenings, letters, website links and other means. Parents will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events through Class Dojo, Tapestry and the school Twitter account
- their children's personal devices in the school

E-Safety Policy

1. **Teaching and Learning**

Internet use is an integral part of the curriculum and is a necessary tool for learning. The school has a duty to provide pupils with good quality internet access as part of their learning experience and recognises a duty to teach pupils how to evaluate internet information and to take care of, and responsibility for, their own safety and security.

The purpose of internet use in schools is to raise educational standards, to promote pupil achievement, develop research skills, to support the professional work of staff and to enhance the school's management functions.

Internet access is an entitlement only for those who show a responsible and mature approach to its use; the school reserves the right to withdraw it if it has concerns about the uses to which it is being put by any individual. Pupils will be taught what internet use is acceptable and what is not, and will be given clear objectives for internet use.

The school will strive to ensure that copying and the subsequent use of internet-derived materials by staff and pupils complies with copyright law. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation; they will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work; and they will be taught to use age- appropriate tools to research internet content

2. Managing Information Systems

- The security of the school information systems and users will be reviewed regularly by the E- Safety Co-ordinator and the ICT Coordinator
- Virus protection will be updated regularly
- Unapproved software will not be allowed in work areas or attached to e-mail
- Files held on the school's network will be regularly checked by ARK ICT Solutions
- There will be a regular review of the school's system capacity conducted by the school ICT network system - ARK ICT Solutions
- The use of user log-ins to access the school's network systems will be enforced

3. Broadband Filtering

The school's broadband access will include filtering appropriate to the age and maturity of pupils. Breaches of filtering will be reported to the E-Safety Co-ordinator. If the breach is such as to constitute a breach of the law, the incident will be reported to appropriate agencies such as Lincolnshire Police, Lincolnshire Safeguarding or CEOP.

If staff or pupils discover unsuitable sites, the URL will be reported to the school's E-Safety Co-ordinator who will record the incident and escalate the concern as appropriate.

4. Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Pupil's Acceptable Use policy and through our E-Safety modules taught through the Rising Stars Coding and Programming package.

5. Personal Data

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.

6. Authorisation of Internet Access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communication systems. Staff will read "Staff Acceptable Use of ICT Policy" and read the Staff Handbook before using any school ICT resources. Parents will be asked to read the school's Acceptable Use policy relating to pupil access, which pupils themselves sign.

All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use policy. Parents

will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, owing to the nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from internet use. Methods to identify, assess and minimise risks will be reviewed regularly by the E Safety Co-ordinator and the ICT Coordinator.

7. Response to Incidents of Concern

All members of the school community will be informed about the procedures for reporting e-safety concerns, such as breaches of filtering, cyberbullying, accessing illegal content. The E-Safety Co-ordinator will record all reported incidents and all actions taken. The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Safeguarding and/or Child Protection concerns, which will then be escalated appropriately. The School will manage E-Safety incidents in accordance with the school disciplinary policies where appropriate. The School will inform parents and/or guardians of any incidents of concern as appropriate. Where there is a cause for concern that illegal activity has taken place then the E-Safety Co-ordinator will report the concern to the police. If the School is unsure how to proceed with any incidents of concern, then the advice of the County E- Safety Officer will be sought. Pupils and parents will be informed of the complaints procedure. Any complaint about staff misuse will be referred to the E-Safety Co-ordinator in the first instance.

8. Cyberbullying

Cyberbullying, as with all other forms of bullying, of any member of the school community will not be tolerated. The school's anti-bullying policy applies in these cases. All incidents of alleged cyberbullying reported to the school will be recorded in the Cyber-bullying Log kept in the Headteacher's Office. Pupils, staff and parents/carers will be advised to keep records of the bullying as evidence. The school will take steps to identify the bully, where possible and where appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, contacting the service provider and, if necessary and appropriate, the police.

Sanctions for those involved in cyberbullying include all those for bullying, as well as potentially:

- The bully may be asked to remove any published material deemed to be offensive or inappropriate;
- A service provider may be contacted to remove content if the bully refuses, or is unable to delete content;
- Internet access within school may be suspended for the user for a period of time

- Parents/guardians will be informed;
- The police will be contacted if a criminal offence is suspected.

9. Managing Email

- All staff and pupils receive a password protected account on arrival at the school
- This should only be used for professional and educational purposes
- Staff and pupils must never communicate using personal email accounts
- All emails must be appropriate in terms of content and tone
- Misuse of the email system could lead to disciplinary action being taken against staff or pupils
- Detailed rules and guidance for staff on email usage can be found in the
- Staff Acceptable Use of ICT policy
- Detailed rules and guidance for pupils on email usage can be found in the
- Pupils' Acceptable Use of ICT policy

10. Managing Social Media

- Teachers wishing to use social media tools with pupils as part of the curriculum should risk- assess the sites before use and check sites' terms and conditions to ensure the site is age-appropriate. If in any doubt, they should consult the School's E-Safety Co-ordinator.
- Staff must not accept current school pupils as "friends" on social media sites. Nor should they discuss the school or pupils of the school on any social media platform.
- Detailed rules and guidance for staff on social media can be found in the Staff Handbook
- The School recognises that social media sites have been used elsewhere by political extremists to radicalise and recruit young people. Our approach is detailed in the following section.
-

11. PREVENT: The Issue of Radicalisation

- The Counter-Terrorism and Security Act 2015, places a legal responsibility on schools to take every effort to protect members of their community from the threat of political radicalisation.

Providing a safe online environment

The federation has strong filters in place to block pupil access to inappropriate materials. Pupils are required to sign up to an Acceptable Use of ICT policy through our Home/School Agreement that specifically prohibits pupils from seeking to access such sites. Internet usage is monitored by a filtering service through ARK ICT Solutions. A cyber-bullying log is kept in school and pastoral and/or disciplinary responses may follow if a pupil's usage breaches our rules or raises concerns. The

School will also seek to block specific sites and search terms too if they appear to pose a risk to our pupils. Furthermore, pupils receive advice and instruction from teaching and pastoral staff on safe internet usage. We use the Rising Stars Coding and Programming software and each unit begins with a session on E-Safety. We also have an E-Safety link on our website.

Staff Training and Information

The School recognises that it has a responsibility to provide INSET to staff on the issue of radicalisation to ensure that they remain vigilant and informed on the issue. It will also ensure staff are aware of how to respond appropriately if concerned about the possible radicalisation of a pupil. Providing a safe online environment

Staff Training and Information

- The School recognises that it has a responsibility to provide INSET to staff on the issue of radicalisation to ensure that they remain vigilant and informed on the issue. It will also ensure staff are aware of how to respond appropriately if
- concerned about the possible radicalisation of a pupil.

Promoting Fundamental Values

- The School will vigorously promote fundamental values such as fairness, democracy, tolerance and the rule of law through its PSHE Programme, its Tutorial Programme, Chapels and Assemblies, the curriculum and all other daily interactions between pupils and staff.

Contacts and Resources

- Government advice to schools on this issue can be accessed here:
- https://www.gov.uk/government/publications/preventing-extremism-in-schools-and- childrens-services
- The Government also provides contact details for alerting authorities to suspected terrorist activity. These include the DfE dedicated telephone helpline and mailbox for non-emergency advice for staff and governors: 020 7340 7264 and counter-extremism@education.gsi.gov.uk in addition to the local police and 101.

12. Mobile Phones and Other Electronic devices

- Detailed rules and guidance for staff on mobile phones and electronic devices can be found in the Staff Handbook
- However, Staff must not give their mobile phone numbers to pupils or seek to contact pupils by SMS “text” messaging

E-Safety Contacts and References

Please also refer to the schools Safeguarding Policy

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Acceptable Use Agreement: Pupils

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with others is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Concerns or clarification may be discussed with the ICT leader.

- I will only use the school's email, internet, intranet, learning platform and any related technologies, including laptops, for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.

- I will not give my personal details, such as mobile number/personal e-mail address, to pupils.

- I will only use the approved, secure e-mail system(s) for any school business.

- I will ensure that personal data (such as data held on MIS software) is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data may only be taken out of school or accessed remotely when authorised by the head of School, Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.

- I will not install any hardware or software without permission of the Head of
- School or Executive Headteacher.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils/staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or staff member. Images will not be distributed outside the school network without permission of the parent/carer, member of staff or Headteacher.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my line

- manager or the Headteacher. I will check all presentations before I use them with pupils.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

- I will respect copyright and intellectual property rights.

- I will ensure my online activity outside school, will not bring my professional role into disrepute. This includes using sites such as Facebook, Twitter and any other social media networks to discuss any school or federation matters.

- I will ensure any social networking within school does not bring my professional role into disrepute. This includes only using sites such as Twitter and any other social media networks to share and promote federation news and information.

- I will support and promote the federation e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

January 2018

Signed……

Mrs CV Collett
Executive Headteacher

Signed……...

Mrs R Blowers
Chair of Governors