Online Safety Policy

for Pupils, Staff, Volunteers and Governors

In the development of this policy consideration has been given to Equality and Diversity and Data Protection.

Equality and Diversity

DEMAT is committed to promoting equality of opportunity for all staff and job applicants. The Trust aims to create a supportive and inclusive working environment in which all individuals are able to make best use of their skills, free from discrimination or harassment, and in which all decisions are based on merit. We do not discriminate against staff based on age; race; sex; disability; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; religion, faith or belief (Equality Act 2010 protected characteristics). The principles of non-discrimination and equality of opportunity also apply to the way in which staff and Governors treat visitors, volunteers, contractors and former staff members.

Data Protection

DEMAT will process personal data of staff (which may be held on paper, electronically, or otherwise). DEMAT recognises the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 (DPA).

This Policy is to be used across all of DEMAT	Version	Date
DEMAT Officer responsible for updating content - DPO	1	April 2018
Date approved by DEMAT Standards & Ethos Committee	1	
Effective date as determined by DEMAT	1	25th May 2018
Notice to be reviewed annually from date last approved by DEMAT Standards & Ethos Committee	1	Annually

Policy Contents

Application of the Policy

This policy is to be used by all employees employed by The Diocese of Ely Multi-Academy Trust (DEMAT). The following definitions are included for reference purposes for both School and Central Team staff to enable clarity and transparency when applying this policy.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Board of Trustees for Central Staff and with delegated responsibility to the LGB (Local Governing Body) for schools

The Board of Trustees has overall responsibility for monitoring this policy for central staff and holding the COO to account for its implementation and with delegated responsibility given to the LGB who has responsibility for monitoring this policy within schools and holding the headteacher to account for its implementation.

Regular meetings will be held with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All LGB members and the COO will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The COO and headteacher

The COO for trust staff and the headteacher for their school is responsible for ensuring that staff understand this policy, and that it is being implemented consistently.

3.3 The designated safeguarding lead for the Trust and Schools

Details of the trust's and school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL for the trust takes lead responsibility for online safety for trust staff, and the DSL for school takes lead responsibility for online safety in the school, in particular:

- Supporting the COO or headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the trust/school
- Working with the COO or headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy or for employees/governors/volunteers through the Acceptable Use Policy for IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices.
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the trust or school to the COO or headteacher and/or the Board of Trustees

This list is not intended to be exhaustive.

3.4 The ICT manager/co-ordinator (the person responsible for ICT at the trust or in school)

The ICT manager/co-ordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils/staff/governors and volunteers safe from potentially harmful and inappropriate content and contact online while at work or school, including terrorist and extremist material
- Ensuring that the trust and school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the trust or school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy for employees/governors/volunteers through the Acceptable Use Policy for IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices.
- This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the trust's and school's ICT systems and the internet (appendix 2), and ensuring that all employees, volunteers and pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy or or for employees/governors/volunteers through the Acceptable Use Policy for IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices.
- This list is not intended to be exhaustive.

3.6 Parents (school use)

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety (school only)

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy or for trust staff the code of conduct policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Employees of the trust, governors and volunteers who are subjected to cyber-bullying from pupils must report this to their line manager immediately who will work with the DSL to investigate, if the cyber-

bullying is from another employee/governor or volunteer they must inform their line manager who will contact the DSL and HR Manager at the trust immediately who will carry out an investigation and where necessary implement the Disciplinary Procedure and Rules relating to misconduct policy.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Trust and school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Trust staff do not have the right to search employees/governors/volunteers personal devices but can remove property owned by the trust/school that is believed to have been used inappropriately. This would be handled under the Disciplinary Procedure and Rules relating to misconduct policy and could result in police involvement.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the trust or school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the trust or school's terms on acceptable use if relevant.

Use of the trust or school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role, please see ICT acceptable use policy for more detail.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils in reception to year 4 are not allowed to bring a personal mobile phone to school. If a pupil is found to have a mobile phone in school in these year groups, the phone will be taken to the school office where the parent/carer can collect it at the end of the day and will be advised that mobile phones are not permitted until Year 5.

Pupils in years 5 and 6 may bring a mobile phone to school if they arrive or leave school alone and the mobile phone is for their safety. All phones must be handed into the school office before the start of lessons and can be collected at the end of the school day, mobile phones should be named and the number logged with the school.

Pupils will not be permitted to use them during the school day or when classed as being in the care of the school. In exceptional circumstances a pupil may request to use their phone by speaking with the headteacher and giving the reason, the headteacher can decide on the action to take.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Employees using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB devices are not permitted, if there is a genuine case for using one a written request must be made to the Trust DPO with the reasons.

If employees have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the trust or school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where an employee/governor/volunteer misuses the trusts or school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the disciplinary procedure and rules relating to misconduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The trust or school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new employees will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All employees will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed yearly by the Board of Trustees. After every review, the policy will be shared with the COO and LGB.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding and child protection policy
- Acceptable use policy – IT/Social Media/Electronic Communications/Mobile Phones/Laptops/Portable Devices
- Positive behaviour policy
- Disciplinary procedures and rules relating to misconduct - employees
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: ICT acceptable use agreement (pupils and parents/carers)

.Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	**School:**

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (employees, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of employee/governor/volunteer/visitor: **Location/work base:**	
When using the trust or school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the trust or school's network using someone else's details	
I will only use the trust or school's ICT systems and access the internet at work, or outside work on a work device, for the purpose of fulfilling the duties of my role. I agree that the trust or school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside work, and keep all data securely stored in accordance with this policy and the trusts data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil or adult informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the trust or school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer: **Location/work base:**	**Date:**
Do you know the name of the person who has lead responsibility for online safety at your place of work?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the trust's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the trust's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing your works ICT systems?	
Are you familiar with the trust's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**