LDBS Academies Trust

Excellence and Equity for All Children in a Christian Context

Teaching Online Safety Policy

INSPIRING BELIEF
in God and one another

ST RICHARD'S
SCHOOL

DATE APPROVED BY THE LAT	May 2020
DATE APPROVED BY THE LAC	May 2020
REVIEW DATE	May 2022
Signed Headteacher	D Hurst
Signed Chair of LAC	Anne [illegible]

Vision Statement

Our schools aspire to provide 'excellence and equity in a Christian context', where every child is valued as a unique individual treasured by a loving God. 'I have inscribed you on the palms of my hands.' Isaiah 49.v16.

Our aim is that every child will have the opportunity to flourish and develop into a rounded adult who can live life to the full. 'I have come that they may have life and may have it in all its fullness'. John 10.v10.

Our schools are places where all are welcome and where we practise kindness and hospitality on a daily basis.

Our vision and our values are clearly displayed and while it is not a requirement that a child and their family have to be practising Christians we do expect all parts of the community, children, staff, parents and carers to support the values that we hold dear.

In our school, we demonstrate how we support this vision through our values, which are Friendship, Endurance, Trust and Hope and summarised in the school's own vision statement: Inspiring belief in God and in one another.

The vision of St Richard's CE Primary School is for a thriving and outstanding school where children and adults, working with the local community, have the opportunity to become the best they can be.

Inspiring belief…

- in ourselves – through progression and fulfilment
- in each other – through motivation and teamwork
- in the children – through showing them their potential
- in the parents – through building trust by results
- in God to all – through our whole lives

- We believe in looking out for everyone
  We put safety first and we do all we can to ensure that all needs are met.
- We believe in working together
  We act like a family who support and motivate one another.
- We believe in aiming for the best
  We do all we can to ensure the highest quality in every area – our children deserve nothing less.
- We believe in looking to the future
  We are positive and seek opportunities to grow and improve, overcoming obstacles to achieve our goals.

We live out our values and vision through our key policies e.g. The LAT Behaviour policy is supported through the values described in the rewards and sanctions section of the policy demonstrating the importance of dignity and forgiveness.

The school admissions policy decided by the Local Academy Committee shows our inclusivity and the importance we place on service to our local community.

The breadth of the curriculum and the creative projects which we enjoy are key to providing opportunities for children to experience life in 'all its fullness', so that alongside learning and wisdom they also experience joy and delight in learning.

Care for the individual and their needs is crucial and the school's policies regarding inclusion and SEND are constant reminders that each of us is known to God and our names are 'inscribed on the palms of His hands'.

LAT HR policies are common in all schools and are created to ensure that individuals are treated fairly and with dignity. All HR policies have been scrutinised by the various unions to ensure that they contain acceptable procedures.

Table of Contents

1. Aims and links with other policies

1.1. The Trust aims to:

- Have robust processes in place to ensure the online safety of all pupils, staff, volunteers, governors, officers and directors.
- Deliver an effective approach to online safety, which teaches and educates all users to protect themselves and make the most effective use of technology across the school.
- Establish clear mechanisms to identify, intervene and escalate any incidents that may be identified.

1.2. This policy should be read in conjunction with:

- Keeping Children Safe in Education Policy;
- Behaviour Policy;
- Disciplinary Procedure;
- Data Protection Policy and Privacy Notices;
- Complaints Procedure;
- ICT User Agreement.

2. Compliance with legislation and guidance

2.1. This policy is based on the following statutory guidance released by the DfE:

- Keeping Children Safe in Education, September 2019
- Teaching Online Safety in Schools
- Preventing and Tackling Bullying and Cyber-Bullying: Advice for Headteachers and School Staff
- Relationships and Sex Education
- Searching, Screening and Confiscation
- Protecting Children from Radicalisation

2.2. Additionally, this procedure meets the standards set within:

- The Data Protection Act
- The Education Act
- The Education and Inspections Act
- The Education (Provision of Full-Time Education for Excluded Pupils) (England) Regulations
- The Equality Act

3. Definitions

For the purposes of this procedure:

Term	Definition
'Board'	Refers to the Board of Directors of the Trust.
'CEO'	Refers to the Chief Executive Officer of the Trust.
'DfE'	Refers to the Department for Education.

'DPL' Refers to data protection law, including the EU's General Data Protection Regulation, the Data Protection Act (as revised from time to time), case law, regulations, and statutory guidance.

'DPO' Refers to the Data Protection Officer.

'DSL' Refers to the Designated Safeguarding Leader at the school, whose details are contained within the Keeping Children Safe in Education Policy.

'ESFA' Refers to the Education & Skills Funding Agency.

'ICT' Refers to information and communication technology.

'ICT Manager' Refers to the ICT Manager, who could be a company under contract by the Trust to provide and / or maintain the ICT services.

'LAC' Refers to the Local Academy Committees of the Trust.

'Trust' Refers collectively to the LDBS Academies Trust and the LDBS Academies Trust 2.

4. Monitoring, evaluation and review of this procedure

4.1. This procedure will be reviewed once every two years, or when the DfE, the ESFA or the Government release new guidance or regulations.

4.2. The DSL should record behaviour and safeguarding issues related to online safety in the incident log, which can be found at Appendix 5.

5. Roles and responsibilities

5.1. The Trust has delegated the overall responsibility for monitoring the implementation of this policy and for holding the (Executive) Headteacher to account over its implementation to the LAC.

5.2. The (Executive) Headteacher should report regularly on the implementation of this policy within their report to the LAC.

5.3. The (Executive) Headteacher should also ensure that all governors and employees working at the school have read and understood this policy and have agreed to use the Trust's ICT systems in accordance with it.

6. Designated Safeguarding Leader's responsibilities

6.1. The DSL's roles and responsibilities are set out in the Trust's Keeping Children Safe in Education Policy. However, in relation to online safety, the DSL is responsible for:

- Supporting the (Executive) Headteacher to ensure that the staff understand this policy;
- Ensuring that the policy is implemented consistently across the school;
- Working with the (Executive) Headteacher to address online safety incidents;

- Logging all online safety incidents;
- Logging and dealing with instances of cyber-bullying;
- Keeping up to date and attending training on online safety;
- Delivering training to school staff on online safety;
- Liaising with external agencies, if necessary, and within the scope of this policy;
- Providing regular reports on online safety to the (Executive) Headteacher and the LAC.

7. The ICT Manager

7.1. The ICT manager is responsible for:

- Putting into place appropriate filtering and monitoring systems, which are updated on a regular basis to keep pupils safe from potentially harmful and inappropriate content and contact online while at school, in line with the latest guidance from the Government, including the Prevent strategy created by the Home Office.
- Ensuring that the ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting security checks and monitoring the school's ICT systems regularly.
- Blocking access to dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are communicated to the DSL to ensure that they are dealt with appropriately.

8. Staff and volunteers

8.1. All staff, including contractors, agency staff, and volunteers are responsible for consistently implementing this policy.

8.2. All staff must agree and adhere to the terms on acceptable use of the ICT systems (see Appendix 3), and ensuring the pupils follow the terms on acceptable use (outlined in Appendix 1 and 2).

8.3. All incidents should be reported to the DSL immediately to ensure that they are logged and dealt with appropriately.

8.4. Staff members 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.

8.5. Staff must ensure that their work device is secure and compliant with the Trust's data protection policies and the DPL.

8.6. All concerns should be raised with the line manager and, where appropriate, with the Trust's ICT Manager.

9. Parents

9.1. The school will work with the parents to raise their awareness of internet safety and will also share this policy with them.

9.2. Parents are expected to notify a member of staff or the (Executive) Headteacher of any concerns or queries regarding this policy.

9.3. All parents should ensure that their children have read, understood and agreed to the terms on acceptable use of the school's ICT systems.

9.4. Parents can seek further guidance from the UK Safer Internet Centre and Childnet International.

10. Visitors and members of the community

10.1. All visitors and members of the community who may use or have access to the school's ICT systems should be made aware of this policy and agree to its terms on acceptable use.

11. Educating pupils about online safety

11.1. 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.

11.2. 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.

11.3. By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships.
- The rules and principles for keeping safe online; how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

12. Cyber-bullying

12.1. Cyber-bullying takes place online, e.g. through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. Please also refer to the school's Behaviour & Anti-Bullying Policy for further information on how instances of bullying will be prevented and addressed by the school.

12.2. The school staff have the power to search for and, if necessary, delete inappropriate images or files from pupils' personal electronic devices, including mobile phones, where they have a good reason to do so.

12.3. 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, disrupt teaching, and / or break any of the school rules.

12.4. If inappropriate material is found on a pupil's personal electronic device, the staff will (in conjunction with the DSL) take an appropriate action, which will involve informing parents and which may involve deleting the material, retaining the material as evidence, and/or reporting it to the Police.

12.5. The Trust will ensure that all searching of pupils is carried out in accordance with the DfE's latest guidance on screening, searching and confiscation.

12.6. Any complaints about searching for or deleting inappropriate material will be dealt with through the Trust's Complaints Procedure.

13. Responding to issues of misuse

13.1. Where a misuse issue has been reported, the Trust will engage the relevant procedure to deal with the issue (i.e. Behaviour & Anti-Bullying Policy and / or the Disciplinary Procedure).

13.2. All actions will depend on individual circumstances, nature and seriousness of the specific incident. If relevant, the school will report the incident to the Police.

14. Training

14.1. All new staff members must receive training, as part of their induction, on safe internet use and online safeguarding issues, such as cyber-bullying and the risks of online radicalisation.

14.2. All staff should receive a refresher training at least once per academic year within the annual safeguarding training. Staff should also be informed of any in-year updates via emails, e-bulletins and staff meetings).

14.3. The DSL and LAC governors should ensure that they undertake child protection and safeguarding training as per the guidance included in the Keeping Children Safe in Education Policy.

Appendix 1 – Acceptable Use Agreement for Early Years and Key Stage 1

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me about, or allowed me, to use.
- Tell my teacher immediately if:
    - I click on a website by mistake;
    - I receive messages from people I do not know;
    - I find anything that may upset or harm me or my friends.
- Use school computers for schoolwork only.
- I will be kind to others and not upset or be rude to them.
- Look after the school's ICT equipment and tell a teacher straight away if something is broken or not working properly.
- Never talk to, or contact, strangers online without permission from a teacher or my parents / carers.
- Save my work on the school computers.
- Check with the teacher before printing anything.
- Log off or shut down the computer when I have finished using it.

I agree that the school will check the websites I have visited and that there will be consequences if I do not follow the rules.

Name: ___________________ Year: ___________________

Signature: ___________________ 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 equipment in school and will make sure that my child understands these rules.

Name: ___________________

Signature: ___________________ Date: ___________________

Appendix 2 – Acceptable Use Agreement for Key Stage 2

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only.
- Only use them when a teacher is present, or with a teacher's permission.
- Keep my private information safe at all times and only share with the permission of my teacher and / or parent / carer.
- Tell a teacher immediately if I find any material which might upset, distress or harm me or others.
- Always log off or shut down a computer when I have finished using it.
- Not access any inappropriate websites.
- Not log in to the school's network using someone else's details.

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

- I will not use it without a teacher's permission.
- I will use it responsibly and will not break the school rules.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Name: ___________________ Year: ___________________

Signature: ___________________ 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 equipment in school and will make sure that my child understands these rules.

Name: ___________________

Signature: ___________________ Date: ___________________

Appendix 3 – Acceptable Use Agreement for Adults (staff, governors, volunteers and visitors)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material.
- 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.
- Install any unauthorised software or connect unauthorised hardware / devices.
- Share my password with others or log in to the school's network using someone else's details.
- Take photographs of pupils without checking with teachers first.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data without authorisation.
- Promote private businesses.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are compliant with the Trust's Data Protection Policy and the data protection law.

I will inform the DSL and ICT manager immediately if a pupil alerts me to any material which might upset, distress or harm them or others. I will also inform the DSL and the ICT Manager of any such material that I encounter.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Name: __________________

Signature: __________________ Date: __________________

Appendix 4 – Online safety training requirements – self-audit for staff

Name of staff member / volunteer:	**Date:**
Question	**Yes / No** (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training / further training?	

Appendix 5 – Online safety incident log

Date	Location of incident	Description of incident	Action taken	Name and signature of staff member