Discovery Schools Academy Trust

Woolden Hill Primary School

Achieving Success, Creating Futures Together

Online Safety policy

Approved by:	Sarah Sadler	**Date:** 02.12.18
Last reviewed on:	15.11.18	**AB Approval:** 03.12.18
Next review due by:	November 2020	**Signed:** S. Lavingia

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and ABMs
- 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 (2018), 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. This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

3. Roles and responsibilities

3.1 General

Effective policies and procedures are in place and updated annually including a behaviour "code of conduct" for staff and volunteers with reference to online safety - "Guidance for Safer Working Practice for those who work with children in education settings October 2015".

An annual safeguarding and wellbeing audit including e-safety is completed by the safeguarding and wellbeing lead professional and outcomes reported back to the Trust Board, Cluster Governing Board and Advisory board through an annual action plan and risk assessment. Headteachers review the Safeguarding and Wellbeing action plan termly. E-safety information is also provided to the Local Authority (on behalf of the LSCB) through the Safeguarding Annual Return.

3.2 Governance

The Advisory board

The Advisory Board will champion issues to do with keeping children safe on line, liaise with the Designated Safeguarding Lead, the Safeguarding and Wellbeing Lead Professional and provide information and reports to the Cluster Governing Board when necessary.

The Cluster board

The Cluster board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Cluster board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Lead Professional for Safeguarding and Wellbeing through the SOAP.

The ABM who oversees online safety is **Louise Mayes**.

All ABMs 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)

3.3 The headteacher

The headteacher is responsible for ensuring that:

- staff understand this policy, and that it is being implemented consistently throughout the school.
- staff receive suitable CPD to carry out their e-safety roles
- there is a culture where staff and learners feel able to report incidents using CPOMS.
- there is a progressive e-safety curriculum in place
- the DSL for e-safety monitors and evaluates incidents pertaining to e-safety across the whole school for children and staff.
- correct DSAT and LSCB procedures are followed in the event of a serious e-safety allegation being made against a member of staff or pupil and informs the Lead Professional for Safeguarding and Wellbeing, Director of IT and CEO about any serious e-safety issues.
- reviews take place of the school's infrastructure/network with the Director of IT to ensure it is as safe and secure as possible and fit for purpose.
- policies and procedures approved within this policy are implemented
- the annual safeguarding audit reviews e-safety with the school's Safeguarding and Wellbeing Lead Professional and actions are planned and accomplished to address any issues which may arise.
- The roles and responsibilities of the DSL for e-safety (as outlined below) are written in their job description and reviewed annually as part of their performance management.

3.4 The designated safeguarding lead for e-safety

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

Mrs Candi Norman takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (CPOMS) 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
- 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 school to the headteacher and/or Advisory board
- Working with the IT lead in school to personalise the online safety curriculum in meeting the needs of the pupils.
- Ensuring that any online safety incidents are logged via CPOMS 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's behaviour policy.

3.5 The IT Technician

The IT technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 school's IT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.6 Lead Professional for Safeguarding and Wellbeing

The Lead Professional for Safeguarding and Wellbeing is responsible for:

- Monitoring and supporting all schools so they meet compliance expectations and are developing online practice.
- Carrying out audits of safeguarding including e-safety arrangements as set out in this policy.

- Supporting schools with parental engagement around online safety.
- Keeping schools informed on developments and updates within e-safety through DSL network meetings.
- Facilitating the delivery of a high-quality curriculum for e-safety, safeguarding and wellbeing in schools.

3.7 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
- They report any suspected misuse or problem to the DSL or DDSL (Deputy DSL) for investigation and implement actions required of them.
- Ensuring that all digital communications with pupils/parents/carers should be open and transparent, on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (CPOMS) 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

3.8 Parents

Parents are expected to:

- Notify a member of staff or the headteacher/head of school 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 IT 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

3.9 Visitors, volunteers and members of the community

Visitors, volunteers and members of the community who use the school's IT 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.

One lesson every half term is based upon the Digital Literacy and internet matters.

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. E-Safety rules will be posted in the ICT suite and/or in all rooms where computers are used and discussed with pupils regularly.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information (Fake news) before accepting its accuracy.

Teachers will teach pupil's to understand and follow the e-safety and acceptable use agreements.

Pupils will be taught to understand research skills and the need to avoid plagiarism and uphold copyright regulations

In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

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

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. 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 for e-safety.

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.)

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. Class teachers will discuss cyber-bullying with their classes, 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, ABMs, advisory board members 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 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. All schools have information on their websites to support the work undertaken on cyber bullying

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.

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. This will be in accordance with the Sexual Violence and Sexual Harassment between children in schools and colleges advice from the DFE.

6.3 Examining electronic devices

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 DSL or Headteacher 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.

7. Acceptable use of the internet in school

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

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governance members 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 may not bring mobile devices into school, unless arrangements have been made for those children who walk home on their own and have to venture beyond the Woolden Hill Estate. If agreement is made, mobile phones are secured in the School Office during the day.

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

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, 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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT technician.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT 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 a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The 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 staff members 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. This will be through the schools own CPD programme which may include a requirement to complete e-safety training through FLIC.

All staff members 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 Deputy DSL's 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.

Governance members 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.

12. Monitoring arrangements

The DSL, Deputy DSL's and/or class teachers will log behaviour and safeguarding issues related to online safety via CPOMS. E-safety incidents are logged using the following categories:

- Social media concern
- Cyberbullying
- Inappropriate searches
- Distributing Obscene images
- Sexting

Child protection records are reviewed regularly by the Designated Safeguarding Leadership Team to check whether any actions are needed. This includes monitoring e-safety incidents such as patterns of complaints or concerns about any individuals and ensuring these are acted upon. Records of these reviews are kept in school (e.g. SLT / DSL meeting minutes, AB meeting minutes).

The Lead Professional for Safeguarding and Wellbeing will collate e-safety records for the SOAP and report this information to the CEO. Where a risk is identified the Lead Professional for Safeguarding and Wellbeing alongside the IT Director will add this to the schools risk register and support the school in addressing this. These risks will be reviewed half termly as part of the schools 'Team around the School' meeting.

This policy will be reviewed annually by the Lead Professional for Safeguarding and Wellbeing and the Director of IT. At every review, any changes to the policy will be shared with the schools, Advisory Board and Cluster governing board as appropriate.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- GDPR
- Complaints procedure
- Social media policy
- Staff handbook (incl. code of conduct)

Appendix 1: 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:	
When using the school's ICT systems and accessing the internet in school, I will: • Use them for a schoolwork or homework • Use them only with a teacher being present, or with a teacher's permission • Not access any inappropriate websites • Not access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Never use chat rooms • Only videoconference call with a teacher present • Never open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use only kind and appropriate language when communicating online, including in emails • Never share my password with others or log in to the school's network using someone else's details • Never give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer • Never arrange to meet anyone offline without first telling my parent/carer, or without an adult to accompany me • 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 (staff, governance members, volunteers and visitors)

Discovery Schools Academy Trust

Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the organisation's computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the organisations systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the organisations ethos, other appropriate policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**
2. Discovery Schools Academy Trust Ltd owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 6 or more characters and is changed regularly.
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from your line manager or the IT Department.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site's (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the IT Department. Any images or videos of pupils will only be used in line with organisational policy and will always take into account parental consent.
7. I will not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access the organisations email system on my mobile device (tablet or mobile phone), the device must be pin or password protected. I will protect the devices in my care from unapproved access or theft.
8. Personal data kept on work devices must be kept to a minimum (examples that **do not** meet this include; Filling the hard drive with music files or photos).
9. I will respect copyright and intellectual property rights.

10. I have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
11. I have read and understood the Loan Equipment policy that covers the use of any staff equipment that I may have been provided in order to carry out my work.
12. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and line manager as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and your line manager.
13. I will not attempt to bypass any filtering and/or security systems put in place by the organisation. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any organisation related documents or files, then I will report this to the ICT Department as soon as possible.
14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.
15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the organisations AUP and the Law.
16. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the organisation I work for into disrepute.
17. I will promote online safety and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on staff member's laptops.
19. I understand this forms part of the terms and conditions set out in my contract of employment.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: …….. Print Name: …… Date: ……

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

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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, ABMs 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? Please record them here.	

Appendix 4: Useful resources for parents

B	BBC Stay Safe	www.bbc.co.uk/cbbc/help/safesurfing
	Becta	http://schools.becta.org.uk/index.php?section=is
C	Care for the family	www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
	Chat Danger	www.chatdanger.com/
	Childnet International "Know It All" CD	http://publications.teachernet.gov.uk
	Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
	Childnet	www.childnet-int.org/
	Cyber Café	http://thinkuknow.co.uk/8_10/cybercafe/café/base.aspx
D	Digizen	www.digizen.org/
F	Family Online Safe Institute	www.fosi.org
I	Internet Watch Foundation	www.iwf.org.uk
	Internet Safety Zone	www.internetsafetyzone.com
K	Kent leaflet for parents: Children, ICT & e-Safety	www.kented.org.uk/ngfl/ict/safety.htm
	Kent Police – e-Safety	www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html
	Kidsmart	www.kidsmart.org.uk/
L	Leicestershire Constabulary – Internet Watch Foundation	www.leics.police.uk/advice/2_information_zone/50_internet_watch_foundation
p	Parents Centre	www.parentscentre.gov.uk
S	Safer Children in the Digital World	www.dfes.gov.uk/byronreview/
T	Think U Know	www.thinkuknow.co.uk/