Delta Federation

Esafety Policy

Approved by:		**Date:**
Last reviewed on:	November 2021	
Next review due by:	November 2023	

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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Caroline Lewis.

All governors 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 headteacher

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

3.3 The designated safeguarding lead

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

The DSL 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 (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

- 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 governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager 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 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 school's ICT systems on a weekly 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

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 school's ICT 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 (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

This list is not intended to be exhaustive.

3.6 Parents

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 is covered in Appendix 3

The safe use of social media and the internet will also be covered in other subjects where relevant. See Appendix 3 for more information.

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, in school presentations or workshops. This policy will also be shared with parents.

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.)

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 tutor groups, 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).

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.

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 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.

7. Acceptable use of the internet and social media

All pupils, parents, staff, volunteers and governors 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, 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.

Parents and pupils are also asked to agree to the school's 'Home/School Agreement' which states that families will 'Not use social media in such a way that causes distress or harm to school / staff or other parents and children'.

8. Pupils using mobile devices in school

Pupils may bring mobile devices with them to school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school
- They must be handed in to the school office at the beginning of the day and collected from the office at the end of the school 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. How the 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.

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

10. 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 biennially by the T&L Committee. At every review, the policy will be shared with the governing board.

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Data protection policy and privacy notices
- Complaints procedure
- Remote Learning Policy

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 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 hand it in to the school office before going to class at the start of the school day • I will collect it from the school office after being dismissed from class at 3:15pm • I will not use it during lessons, tutor group time, 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: 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**

Appendix 3: Child Focused E-Safety Protocol

1. 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:

- To know there are unfamiliar people online and to consider them unsafe
- To treat others online kindly and with respect
- Use technology safely and respectfully, keeping personal information private
- Know 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:

- To ensure personal and private information is never shared online
- Use technology safely, respectfully and responsibly
- To show and promote kind and respectful treatment of others online
- Consider the digital footprint a user leaves online
- Recognise acceptable and unacceptable behavior in a variety of digital environments
- Identify and use a range of ways to report concerns about content and contact
- To share and encourage other students to use safe and responsible practices online

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.

Pupils will complete a half term unit of e-safety related learning each school year. This may be embedded within other learning or discreetly taught as a specific unit of work.

E-Safety is the responsibility of everyone in and around the school community. The role of the safeguarding team is to support and lead all members of the community in safe and responsible online activity.

Responsible and Respectful

Children are expected to learn about and embody a responsible and respectful attitude to all online behavior, in and outside of school. This mentality will be developed through discreet teaching, modelling by teachers and older peers and a narrative of appropriate activity and behavior within assemblies, safer internet week and daily practice in classroom settings.

Data Protection and Privacy

Children will be taught to understand that some information and data is private and should not be shared. It is crucial children know what data is private to them and others so they can protect themselves at all times. Children need to be encouraged to consider their own digital footprint and the traces their activities leaves online. Consequently, children must know what to do, or be supported in acting, should any loss or accidental sharing of theirs or someone else's data.

Privacy is critical in protecting one's personal data, this must be explicit to children throughout any discreet teaching or information pertaining to online safety. Children will be encouraged to always maintain the highest levels of any privacy settings online; as part of any account; activity or use of websites. It is important that this is reflected by all staff, as per the *Brooksward School Online Safety Policy.*

Cyberbullying

Children will be taught the definition of Cyberbullying as it appears in the *Brooksward School Online Safety Policy* and will be made aware of how to raise concerns with school staff should they be involved in any such incident. They will also be made aware of how situations will be dealt with, as per the *Brooksward School Behaviour Policy.*

Age Restrictions

It is expected that children comply with age restrictions and recommendations in place on all websites and digital media for use online (including, but not limited to: social media websites, YouTube, email accounts, PlayStation Network, Microsoft XboxLive, computer and console games, videos, Blu-Ray, DVD). Parents and carers should be asked and encouraged to support the school community in adhering to any age restriction relating to online content and activity. Issues relating to children's non-compliance to any age restriction or recommendation will be dealt with as per the *Brooksward School Behaviour Policy*.

Appendix One

We ask all of our families to sign a copy of the Remote Learning Agreement

Remote Learning Agreement - children who are working remotely and in school

We ask all children, young people and adults involved in the life of Brooksward School/Drayton Park School to sign this Remote Learning Agreement to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your children should not behave any differently when they are out of school or using their own device or home network than they would in the classroom whilst completing remote learning.

The rules around behaviour and respect for pupils applies to all members of the school community, whether they are at home or school whilst they are carrying out their learning.

You can read the full Remote Learning Policy on our website for more details on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this RLA or our approach to online safety, please contact the school.

Parent/carers and each child must read the following guidance and agree to the conditions.

Parent/Carer Agreement

1. I understand that Brooksward/Drayton Park School uses technology as an approach to their remote learning whilst pupils are unable to attend school.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements and internet safety education. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies at home, which can sometimes be upsetting.

3. I understand that the video and microphone will be on and others on the virtual session will be able to see and hear my child when we are engaged in a class group session.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, pupils or other parents/carers.

5. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.

6. I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed. When on any live video calls with school, my child will be fully dressed and in a space where there are able to concentrate, a clear background and the camera angle will point away from any personal information/photographs etc. Where it is possible to blur or change the background, I will help my child to do so.

7. I understand that whilst home networks are much less secure than school ones, I can apply child safety

settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk

8. I understand that I am responsible for supervising my child's access to virtual calls and will monitor my child during this time and take responsibility for their conduct. I understand that I am not part of the learning session and will be there to support my child with their technology, where appropriate. I will ensure that they are ready for their live learning session.

9. I understand that each virtual meeting will end at the discretion of the teacher and that children may face future sanctions such as being blocked or removed from calls if they do not follow this agreement.

10. I understand that virtual sessions will be recorded by class teachers and may be saved according to data protection guidelines and safeguarding.

11. I understand that I must not take any photographs or videos of the live session myself.

12. I understand that teachers or support staff will lead and facilitate all virtual meetings and that classroom behaviour and rules will be followed by my child during this time.

13. I understand that I must maintain confidentiality of the content of the virtual sessions and not share any information about it verbally or online.

14. I understand if I am concerned about anything that happens in the live session, I must report it to the class teacher or Head.

Child Agreement

Please share this with your child so they know what they must do to keep themselves safe online.

1.When I learn online – I use technological devices and logins for remote learning, other activities and having fun. All of my devices and systems are monitored by an adult when I'm using them at home.

2. When I am completing my home learning, I follow the school values

3. I will only use devices, apps, sites and games that are age appropriate when I am allowed to.

4. I am a friend online – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

5. I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

6. I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

7. I ask for help if I am scared or worried by something I see– I will talk to a trusted adult if anything upsets me or worries me on an app, site or game.

When I am on live learning sessions I will:

- be ready to learn including going to the toilet before the session
- dress appropriately

- I am in a safe and calm place at home which is a suitable space for my teachers to call me in.

- I will follow the school values at all times and use kind words towards others during calls.

- I will listen and follow the instructions of the class teacher during calls in the same way I would in the classroom.

- If I have a question, my teacher will let me know how I can do this

- I will be ready for my learning with the resources I need (paper, pencil, online resource)

- I will complete all work set as well as I possibly can

If I have any questions about this, I will ask my family or teacher.

Child Agreement: I have shared this with my child and they have understood this agreement

YES

Child Name

Parent/Carer Agreement: I have read and agree to all terms

YES

Adult Name

We ask all parents to sign a copy of the following agreement :