Frederick Bremer School

E-Safety Policy

Person Responsible	Fenella Hewitt
Review Frequency	Every 3 years
Last Reviewed	January 2023
Does this policy need to be ratified by Governors?	Yes
If yes, which committee	SIP
Ratified by Governors on	31st Jan 2023
This policy is communicated by the following means	Information Hub and School Website

Contents

1. Aims

Frederick Bremer 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- 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

It also refers to the DfE'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.

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 coordinate 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 Michelle Hegarty, Safeguarding Governor.

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
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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.

The Headteacher at Frederick Bremer School is Jenny Smith.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and the Designated Safeguarding Team are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy

- Ensuring that any online safety incidents are logged on sims and CPOMs if appropriate and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- 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.

The Designated Safeguarding Lead at Frederick Bremer School is Fenella Hewitt (Deputy Headteacher).

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 daily 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 on sims or CPOMs where appropriate 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.

The Network Manager at Frederick Bremer School is Tony Akinbule.

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 and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers 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

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

- What are the issues? – UK Safer Internet Centre and National Online Safety
- Hot topics – Childnet International and National Online Safety
- Parent resource sheet – Childnet International and National Online Safety

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.

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

At Frederick Bremer the topic is also taught through our discreet curriculum on drop down days for example and through the assembly plan

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 or google classroom. This policy will also be shared with parents via our website.

Online safety will also be covered during parents' information sessions and at other appropriate opportunities.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 1 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. Form tutors will discuss cyber-bullying with their tutor groups and it is covered through the assembly program.

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.

In line with Frederick Bremer's relational behaviour model and holistic approach ti behaviour, the school puts support in place for perpetrators as well as victims, this will be bespoke to the child, family and incident. This may be through open and transparent meetings, emotional literacy support, social stories linked to kindness, safer school support to give some examples.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search of an electronic device, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent/necessary the search is, and consider the risk to other pupils and staff. If the search is not urgent/necessary, they will seek advice from the DSL or a Deputy DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team] to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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 families are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). 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 appendix 1 for families

8. Pupils using mobile devices in school

Mobile phones are not allowed to be used in school, if they are seen or heard they are confiscated. Mobile phones will not be handed back to the child but to and parent or carer or nominated adult as set out in the school behaviour policy

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in staff induction training

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school's Network Manager.

10. 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 our behaviour policy. Internet misuse is managed on a case by case basis. 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 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 staff disciplinary procedures and staff code of conduct. 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.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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 via CPOMs

This policy will be reviewed every year by the Deputy Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1:

Frederick Bremer School ICT Parental Consent & Agreements – An Explanation for Parents found in parent handbook

The information below is provided to parents and carers to help with understanding the context surrounding each of the consent requests made by the School. Please ensure that you use this information in conjunction with our standard 'Consent Form' when providing / declining your consent within each of the given contexts.

Section 1: Using Photographs

As part of the information we use to support your child's education, we hold a copy of their photograph as part of their electronic file within our computer system. These photographs are held securely and used within the school to assist staff with administrative processes, such as the identification of individual pupils and within our planning and assessment systems.

Alongside these administrative purposes, there are also a number of instances in which we would like to use photographs of pupils which have been taken within the school or during school organised activities, for which we require parental consent.

Internal Displays: Photographs of pupils are used within our internal displays to highlight participation within specific learning activities as well as to celebrate the achievements of individual / groups of pupils.

Photographs used within this purpose may be viewed by anyone within the school including pupils, parents, staff and also visitors from outside the school community.

School Newsletter: Photographs of individuals and groups of pupils are used within our School Newsletter to inform the school community about the activities which our pupils have been involved in as well as celebrate specific achievements across the school. This newsletter is shared with members of the school community and is published on the school website.

Website/Social Media: Photographs of individuals and groups of pupils are used within information published on the school website and through the School's social media channels. These are used within information about the activities that pupils have participated in, to celebrate the achievements of individuals/groups of pupils and also within general information published about the school. School Prospectus/Publicity material: Photographs of individuals and groups of pupils are used within our prospectus and printed/electronic publicity materials in order to promote the school in general as well the activities which our pupils are participating in. Our prospectus and promotional materials are shared with a wider audience, including current/prospective parents, community organisations and visitors to the school.

Section 2: School Publicity & Marketing Material

As a school we are keen to ensure you are aware of the activities that take place across the school and are kept up-to-date with the achievements of pupils. We will always keep you up-to-date with matters that relate to your child’s education and inform you of events that they can participate in / are involved in but require your consent to provide you with further information about events and achievements across the school.

School Newsletter: As a school we publish a half-termly newsletter which provides an overview of the activities that have taken place within the school and to celebrate the achievements of our pupils. Copies of each edition of our newsletters are shared electronically with parents via School Gateway using the email address provided.

Promotional Material: We are keen to inform parents of other events that take place within the school and to provide details of any appropriate marketing material. Copies of any applicable information / material will be shared electronically with parents via School Gateway using the email address provided.

Section 3: Other consents not relating to the use of personal information

As a school we believe that ‘Educational Visits’ play an important role in learning and we are, therefore, keen to provide your child with opportunities to learn outside the classroom. To enable your child to take advantage of opportunities outside the school premises we would like to take this opportunity to confirm parental consent for their child to participate in these activities.

Off-site PE activities: Within our PE curriculum we make use of a number of additional specialist sporting facilities within the local area to help enhance our lessons where specialist facilities may be required. All lessons which make use of external facilities will commence at Frederick Bremer, following which pupils will be escorted to the relevant venue by members of school staff. Following completion of their lesson, pupils will be escorted back to the school to continue their other remaining lessons but please note that pupils will be dismissed directly from any external PE venue at 3pm if their lesson finishes at the end of Period 6. Educational Visits within the School’s ‘Educational Area’: The majority of our educational visits take place within our ‘Educational Area’ (defined as “the local area (defined as “the area within 30mins walk of the school and all recognised establishments within zones 1-4 of the London Transport travel zones”) and take place within the School’s normal operating hours.

In instances where your child will be participating in any such activity we will ensure that you are aware of all relevant details but will not trouble you with a requirement to provide your consent to each individual activity. Your consent will still be sought in instances
where you child will be participating in any educational visit which operates outside these parameters or involves any adventurous/higher-risk activity.

Section 4: Acceptable use of ICT Agreement

As part of the school's Information and Communications Technology (ICT) programme, we offer pupils 'supervised' access to a range of ICT resources, including the internet and a school email. To ensure that these
resources are used safely and constructively we have outlined a series of restrictions and protocols in our 'Acceptable Use of ICT Agreement'. Acceptance of this agreement is required in order for us to provide your
child with access to ICT resources within the school.

Changing your consent in the future

If you change your mind about consent, you can withdraw your consent at any time by emailing
school@bremer.waltham.sch.uk or via your School Gateway account.

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**