Frederick Bremer School

E-Safety Policy

May 2020

Person Responsible	Alex Palombo
Review Frequency	Every 3 years
Policy First Issued	April 2020
Last Reviewed	September 2020
Agreed by LT on	n/a
Does this policy need to be ratified by Governors?	Yes
If yes, which committee	SIP
Ratified by Governors on	7/10/20
This policy is communicated by the following means	Information Hub and School Website

Contents

1. Policy Aims

The internet and digital technologies are integral parts of the lives of our 21st century children. The ability to access and exchange information from anywhere has many educational and social benefits but ensuring that it is used appropriately by children and young adults can often be challenging for us all. E-Safety and ensuring the safety of our pupils when operating online are, therefore, fundamental elements of our safeguarding responsibilities. In fulfilling these responsibilities our school E-safety approach aims to:

- Provide an approach to online safety, which protects all users both in and out of school
- Develop processes that enable users to understand, identify and manage any potential risk faced whilst online
- Establish clear processes to identify, intervene and manage any incident/concern, which might arise.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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
- Searching, screening and confiscation

It also refers to the Department for Education'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 Body

The governing body has overall responsibility for monitoring this policy and ensuring its effective implementation across the school. Within the governing body, the SIP Committee holds responsibility for overseeing this policy and its related process.

All governors will:

- Ensure that they have read and understand this policy and the processes defined with it
- Adhere to the acceptable use conditions which apply to use of the school's ICT systems and internet services (appendix 3)

3.2 The headteacher

The headteacher has overall responsibility for ensuring that all staff understand this policy, and that it is implemented consistently throughout the school.

3.3 The designated safeguarding lead

The Designated Safeguarding Lead has overall responsibility for E-Safety across the school. Specific responsibilities within this remit include:

- Supporting the headteacher in ensuring that staff understand this policy and that it is implemented consistently throughout the school
- Assessing any relevant staff training needs and ensuring that this is planned and delivered effectively to relevant staff
- Working with the headteacher and other relevant staff, as necessary, to identify and address any E-Safety issues or incidents
- Ensuring that any E-Safety incidents are recorded and responded to/managed appropriately in line with this policy (See section 10 of this policy for details of the required recording process)

- Ensuring that any incidents of cyber-bullying are logged via CPOMS, and dealt with appropriately and in line with the school behaviour policy and its associated processes
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

Details of the Designated Safeguarding Lead (and Deputy Designated Safeguarding Leads) can be found in our Safeguarding Policy and are displayed on Safeguarding posters in every classroom.

3.4 The ICT Network Manager

The ICT network manager is responsible for:

- Ensuring that appropriate filtering and monitoring systems are in place (including regular updates) in order to keep pupils safe from potentially harmful and inappropriate content whilst in school and/or using school ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting relevant security checks and monitoring the school's ICT systems to ensure that these are appropriately protected and protect users accordingly
- Ensuring that the Designated Safeguarding Lead is informed of any E-Safety incidents that are identified and providing any necessary support or information whilst incidents are managed

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including agency staff and volunteers, have a shared responsibility to ensure the school achieves the aims set out in this policy. Specific responsibilities within this policy include:

- Ensuring they are aware of all elements of this policy as they apply to their individual role within the school
- Implementing this policy consistently
- Adhering to the acceptable use conditions which apply to use of the school's ICT systems and internet services (appendix 3)
- Ensuring that pupils use the school's ICT systems safely and in accordance with the requirements of the acceptable use of ICT agreement (appendix 2)
- Ensuring that any E-Safety incident/concern is reported and that the Designated Safeguarding Lead (or nominated member of staff) is supported in their response to/management of this incident.
- Ensuring that any incidents of cyber-bullying are logged via CPOMs, and that all appropriate actions are taken to support the school's response to such incidents

This list is not intended to be exhaustive.

3.6 Parents and Carers

Parents and carers play a vital role in supporting their child's safe use of ICT systems and are also asked to support the school in achieving the aims set out in this policy. Within the framework of this policy, parents and carers are expected to:

- Ensure their child has read, understood and adheres to the requirements of the acceptable use of ICT agreement (appendix 2)
- Inform the school if their child is affected by any incident/concern associated with E-Safety, including any instance of cyber bulling should this occur

Further details of support and advice which is available to parents and carers can be found in our Parent Handbook and is available through our website.

3.7 Pupils

Pupils have a responsibility to ensure they act appropriately at all points when using the school's ICT systems and infrastructure. In particular, pupils are expected to:

- Ensure they adhere to the requirements of the acceptable use of ICT agreement (appendix 2)
- Ensure that their actions and conduct do not affect access to the school's ICT subsystems and infrastructure if it's use by others.
- Ensure they actively participate in all E-Safety related learning activities and make efforts to use information, advice and guidance provided to enable their safe use of ICT
- Inform the school if they are affected by any incident/concern associated with E-Safety, including any instance of cyber bulling should this occur

This list is not intended to be exhaustive.

3.8 Visitors and members of the community

Visitors and members of the community who might use the school's ICT systems will be made aware of this policy, when relevant, and are expected to adhere to it appropriately. If appropriate, visitors and members of the community will also be expected to adhere to the acceptable use conditions which apply to use of the school's ICT systems and infrastructure.

4. Educating pupils about online safety

Promoting the safe use of technology and the internet is an important element of our approach to E-Safety. Pupils, therefore, receive information, advice and guidance which relates to elements of E-Safety within a range of subject areas. Specific focused learning elements are also completed within the following subject areas:

- Computing
- Legal & Social Studies
- Wellbeing

Focused learning within these curriculum aims to ensure that pupils develop the following competencies during their time at the school:

- Develop an understanding of a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Develop an understanding of how to recognise inappropriate content, contact and conduct, and know how to report and seek advice if concerns arise
- Develop an understanding of 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
- Develop an understanding of individual rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Develop an understanding of how changes in technology affect safety, including new ways to protect their online privacy and identity

Full details of how these aims are mapped across the curriculum can be found within Appendix 1 of this policy.

5. Information and Support for Parents

The school aims to ensure that parents and carers have access to appropriate sources of information to enable them to understand the issues associated with E-Safety and to enable them to effectively support their child's safe use of ICT technology.

We acknowledge, however, that some parents and carers may feel that they already have a clear understanding of these concepts and that they may already be confident in the methods they use to ensure their child's safe use of ICT. Within this policy therefore, the school adopts a 'supportive' position and will make information and sources of support available to all parents for them to access and digest as and when they feel it is necessary - Full details of the sources of advice and support available to parents can be found in Appendix 4 of this policy.

If parents or carers have any queries or concerns in relation to E-Safety, then we would also be happy to provide any personalised support required – Please contact your child's form tutor, head of year or a member of the safeguarding team if you would like to discuss any specific queries.

6. Cyber-bullying

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. The school takes all forms of bullying seriously and manages its response to any bullying that might take place within the processes set out within out Behaviour Policy.

6.1 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, the school aims to ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We work hard to ensure that all pupils are able to identify any instance of cyber bulling that might occur, and that they have the skills, confidence and belief to report concerns via an appropriate channel.

To achieve this aim, the school will actively discuss issues associated with cyber-bullying within the curriculum, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Additional information, advice and guidance will also be provided to pupils as may be appropriate to support them in understanding any additional/emerging risks that might occur.

All staff, governors and volunteers (where appropriate) receive advice and training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to any instance where cyber-bullying is identified, the school will address this in accordance with the principles and processes set out in our 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.

7. Acceptable use of the ICT in school

All ICT users (including pupils, staff, governors, agency staff and volunteers) are expected to adhere to the relevant acceptable user agreement – See Appendix 2 & 3 for further details.

The school actively monitors adherence to these acceptable use agreements and reserves the right to restrict (or prevent) access to the internet and/or ICT systems for any user identified as not adhering to the conditions within these agreements.

8. Personal electronic devices in school

8.1 Pupils

Pupils are not permitted to use personal electronic devices (including mobile phones, tablet/laptop computers, games consoles, etc) at any point whilst in school.

Whilst we understand that parents and careers may prefer that pupils have access to a mobile phone during the journey to/from school, the school considers these devices as 'Banned Items' and, in accordance with our behaviour policy will take steps to confiscate any such item used or seen in school.

8.2 Staff, Governors and Volunteers

All staff (including agency staff and contractors), governors and volunteers must ensure that their use of any personal electronic device complies with the requirements established within the code of conduct and in adherence with all relevant safeguarding guidance provided.

8.3 Parents & Visitors

The school understands that parents and visitors are likely to bring personal electronic devices when visiting the school. Parents and visitors are asked to restrict the use of any personal electronic device whilst in school, and are reminded

that they may not be used to photograph, video or record any element of their visit (unless specific consent is provided an advance by a member of school staff).

8.4 Examining electronic devices

The school has specific powers within legislation (Education and Inspections Act 2006 and Education Act 2011) to search for and, if necessary, delete inappropriate cornet stored on pupils' electronic devices (including mobile phones, tablets and other electronic gadgets), where staff believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine 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/learning, 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 Headteacher or Designated Safeguarding Lead to decide whether the school should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline), and/or report it to the police.

Any decision to search and any resulting search of electronic devices will be completed in accordance with the school's established search protocols and, by inference, in accordance with the relevant Department for Education guidance.

8.5 Liability for personal electronic devices

The school accepts no responsibility for theft, loss or damage to any personal electronic device brought into school. Any member of the school community who chooses to bring a personal electronic device into the school does so at their own risk.

9. Staff using work devices

Staff members using a work device outside school must not install any unauthorised software on the device and should use this device in accordance with the school's acceptable user agreement at all times (see appendix 3 for further details).

All school devices are password protected and staff must ensure that they do not share passwords with other people. Individual staff members using school devices should always take all reasonable steps to ensure the security of the device and its contents and be particularly mindful when using it outside school.

If staff have any concerns regarding the security of their work device, they must seek advice from the ICT network manager immediately.

10. Responding to concerns

The school takes E-Safety seriously and will respond to all incidents of concern that are identified by the school or reported to us. Owing to the diverse and rapidly changing nature of ICT and internet usage this policy does not intend to provide specific responses that will be employed. Details below provide a reminder of the required reporting processes for use by staff along with an outline of the likely response process:

Identified/reported Concern	Recording Process	Response Process
Concern relating to a pupil's use of ICT systems or the internet within the classroom (e.g. Attempting to access restricted content)	All such concerns should be reported to the classroom teacher and recorded on CPOMS	Initial Response actioned by the classroom teacher in accordance with the behaviour policy. Additional support or action might be provided by the Designated Safeguarding Lead.
Concern arising from negative or inappropriate interaction between pupils via social networking (e.g. Cyber bulling,	All such concerns should be recorded on CPOMS immediately	Response actioned by the child's head of year. Additional support

requesting/sharing inappropriate content, etc)		or action might be provided by the Designated Safeguarding Lead
Serious concern relating to online actions directed towards a pupil by others (e.g. Serious threats, grooming, exploitation, etc)	All such concerns should be recorded on CPOMs immediately. Additional records will be kept by the DSL within the E-Safety Incident log.	Full assessment of the incident required, following which the response will be managed by the Designated Safeguarding Lead in accordance with the relevant process.
Other concerns (e.g. Inappropriate content accessible despite filtering)	All such concerns should be reported to the DSL immediately.	Full assessment of the concern is required, following which the response will be managed by the Designated Safeguarding Lead.

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

11. Training

The school is committed to ensuring that all staff have access to and complete any training necessary to enable them to effectively and confidently fulfil their roles. To achieve the aims of this policy, the school provide training for staff as follows:

- **New Staff**: All new staff receive E-Safety training as part of their induction. This introduces the core issues covered within this policy (e.g. Cyber bullying) and covers factors associated with safer working practices as well as wider online safeguarding issues (e.g. online radicalisation).
- **All Staff**: All staff receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (e.g. through emails, staff bulletins and staff meetings).
- **Designated Safeguarding Training**: The Designated Safeguarding Lead, Deputy Designated Safeguarding Leads and other pastoral staff will undertake extended safeguarding training which includes E-Safety. Staff with Designated Safeguarding Training are available to support other staff with advice and guidance if required.
- **Governing Body**: All governors receive basic safeguarding training which includes elements of E-Safety and safer working practices.
- **Volunteers**: Volunteers will receive appropriate training and updates, if applicable.

Additional training and recommendations of further sources of support are available to all staff (on request) via the Designated Safeguarding Lead and Deputy Designated Safeguarding Lead responsible for E-Safety.

12. Monitoring arrangements

This policy will be reviewed every three years by the Designated Safeguarding Lead and/or Deputy Designated Safeguarding Lead with responsibility for E-Safety. Following each review process, this policy will require ratification by the governing body.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- GDPR Policy
- Acceptable use of ICT agreements
- Staff disciplinary procedures

- Complaints procedure
- Child Protection and Safeguarding: COVID-19 Addendum to Safeguarding Policy (April 2020)

Appendix 1: E-Safety Within the Curriculum

Pupils receive information, advice and guidance which relates to elements of E-Safety within a range of subject areas. Specific focused learning elements are also completed within the following subject areas:

E-Safety learning within the Computing Curriculum

School Term	Year Group	Focus
Autumn Term	7	**Basic Concepts**: Pupils develop their understanding of how to use computers safely, effectively and responsibly (including looking at file management and security). **Keeping Safe**: Pupils explore the concepts associated with e-safety and online profiles in order to promote an understanding of how to ensure safe and responsible use of social media and management of online profiles. **Understanding Dangers**: Pupils investigate the possible dangers associated with using social networking sites, including issues such as cyberbullying, inappropriate content and potential grooming). **Responding to Concerns**: Pupils develop their skills and understanding of how to respond safely to a range of concerns that might arise whilst using social networking sites.
Spring Term	8	**Legal Frameworks**: Pupils investigate a range of legislative controls associated with the use of computer technology, including exploring their implications on the use of computers and technology. **Cyber Security**: Pupils investigate the issues associated with several potential cyber scams, including "Phishing", "hacking", "data harvesting" and "identity theft". **Impact of Technology**: Pupils explore a range of ethical, safety and environmental issues associated with the production, use and disposal of computers and digital devices are also discussed.
Summer Term	9 and 10	**Data Security**: Pupils develop a wiser understanding of the concepts associated with data security, including exploring the differing security needs and methods associated with a range of different data types. **Personal Security**: Pupils further investigate the issues associated with personal security and exposure to cyber scams, including understanding the legal frameworks associated with social networking and social media.

E-Safety learning within the Wellbeing Curriculum

School Term	Year Group	Focus
Autumn Term	10	**Digital Footprints** – Pupils explore the issues associated with creating their online identity, including consideration of how their personal data/information may be accessed/used and steps they can take to keep it safe.
Spring Term	8	**Cyber Ethics** – Pupils develop their understanding of ethical behaviour whilst online, including detailed exploration of the issues surrounding positive communication and cyber-bullying.
	9	**Staying Safe**: Pupils further develop their understanding if safe and ethical use of online platforms, including investigation of the issues/consequences around personal profiles, revenge positing catfishing.
	10	**Inappropriate Content**: - Pupils explore the issues, legal frameworks and consequences associated with accessing/sharing inappropriate content whilst online, including links to data security/caner bullying.
Summer Term	7	**Staying Safe**: Pupils develop their understanding of appropriate/inappropriate sharing of martial and information whilst online, including consideration of how to manage peer-pressure, expectations and personal identity.

Appendix 2: Acceptable User Policy – Pupils and Parents/Carers (Computer facilities including use of the Internet)

Rationale

ICT facilities have tremendous potential for education but they need to be used appropriately.

As part of the school's curriculum and at other points within the school programme we offer pupils supervised access to ICT systems and the Internet. Access to the Internet will enable pupils to explore thousands of libraries and databases. In spite of the tremendous potential for good that is available, you should be advised that some material, accessible via the Internet, contains items that are illegal, defamatory, inaccurate or potentially offensive to some people. The Internet Provider, Cyber sitter software and the web caching box which we use in school provides a service which prevents most access to such material. However, no filtering service can be completely fool proof.

Whilst our aim for ICT and Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. In school, teachers will guide pupils toward appropriate material and do all they can to ensure pupils do not access undesirable sites. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantage. But ultimately, parents and carers are responsible for setting and conveying the standards that their children should follow when using media for information sources.

Principles

- Access is a privilege, and pupils are responsible for good behaviour and positive digital footprints on the school network and the Internet.
- Pupils are not allowed to have unsupervised access to computers or the Internet.
- The school can and does track information on work carried out on computers and sites visited on the Internet.
- Parental support is sought for upholding high standards.
- Pupils and parents/carers are required to sign an agreement, which they must honour.

Rules for Pupils

Most Internet use will be clearly defined as part of a lesson. Outside of this, you may have other opportunities to use the Internet, e.g. Homework Club. These may apply to all situations and may also apply to home or outside school use.

1. You must only access those services you have been given permission to use.
2. You must **not** access the service without a supervisor. A supervisor can either be a teacher or the LRC Manager or other adult that is employed in the school.
3. Any work/activity on the Internet must be directly related to your school work.
4. Do **not** disclose any password or login name you have been given to anyone. Change your password immediately if you believe someone else has your details.
5. Do **not** give your personal information to anyone. Under no circumstances give addresses/telephone numbers of any teachers and pupils at Frederick Bremer School. Use of names of pupils or photographs of pupils is forbidden.
6. Do **not** download, use or upload any material or use material which is copyright.
7. Do **not** download/upload any software on to the school network.
8. Do **not** damage computers, computer systems or computer networks.
9. Do **not** trespass in another user's folders, work or files.
10. Do **not** give your name/password to another user or adult.
11. Do **not** post anonymous or personal communications.
12. Do **not** waste resources (such as on-line time, paper).
13. Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist, or inappropriate sexual content. If you are not sure about this, or any materials, you must ask your supervisor.
14. You must agree for the systems supervisor to view any material you store on the school's computers, or software you use on the school's computers.

15. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do **not** use computer systems to threaten, scare or bully any other member of the school. Do **not** state anything, which could be interpreted as libel.

Failure to comply with these rules will result in one or more of the following:

A. A ban, temporary or permanent, on the use of ICT and/or Internet facilities at school.
B. A letter informing your parents of the nature and breach of rules.
C. Appropriate sanctions and restrictions placed on access to school facilities to be decided by the Head of Year/Head of Department.
D. Any other action decided by the Headteacher and Governors of Frederick Bremer School.

Sanctions

- Violations of the above rules may result in a temporary or permanent ban from the facilities.
- Disciplinary action will be taken in line with the school's discipline policy; this may include detentions and in serious cases fixed term exclusion.

For serious breaches of the above rules, the police may be involved.

Further details are provided to all pupils and parents and are available on the school website. Please see senior staff if you are unclear about any aspect of the policy.

If you do not understand any part of this Acceptable User Agreement, you must ask an appropriate member of staff for further clarification.

May 2020

This agreement is reviewed regularly and updated to ensure the most effective use of ICT in the school. We will notify parents/carers of any changes and publish this on the school website.

Appendix 3: Acceptable User Agreement (Staff inc. governors, volunteers and visitors)

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such 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, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand 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 secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Advice and Sources of Further Support for Parents & Carers

The internet and digital technologies are integral parts of the lives of our 21st century children. The ability to access and exchange information from anywhere has many educational and social benefits but ensuring that it is used appropriately by children and young adults can often be challenging for us all.

General Advice for Parents and Carers

As a parent or carer, you will of course decide what is right for their child but general advice and guidance from the key internet safety organisations includes the following:

- Helping them to understand the potential risks associated with social networking (e.g. having many online 'friends' might mean your child may be revealing personal information to complete strangers).
- Ensuring they always set their social network profile settings to private and keep their personal information private.
- Encouraging them to think about who their online 'friends' are, remind them not to arrange to meetup with someone they only know online and tell you if someone asks.
- Encouraging them to think before they post, send or forward any content online as they need to be aware that they cannot control its distribution once posted.
- Regularly discussing with them the kind of websites that they use, how to set safety features and how to report concerns.
- Ensuring that they feel happy and safe when online and that they do not feel pressured into sharing or accessing inappropriate content.
- Ensuring they do not have access to use your credit card or bank details whilst they are online
- Ensuring that they know they can discuss anything that happens online which worries or upsets them and that you will support them to resolve the issue

It is worth remembering that children do not always fully consider the risks and can often be concerned that they will lose access to the internet if they reveal they have got into trouble online. It is, therefore, important to ensure that these things are regularly discussed to make sure that your child feels that they can raise any concerns with you.

Reporting Concerns

Parents and pupils are strongly recommended to report any concerns they have in relation to activity online. As a school we will always support with resolving issues involving other pupils and can signpost other appropriate sources of resolving issues which do not involve other pupils from the school. The majority of website and apps also contain a "Report It" function which can be used to alert providers and/or CEOP of other serious concerns. The following information is provided as a guide to help you identify the most appropriate method of reporting concerns:

Summary of concern	Recommended Reporting Process
Your or your child have a concern about online actions or behaviour involving pupils from the school (e.g. cyber bullying, requesting/sharing inappropriate content, etc)	We recommend you contact the school and discuss the concerns with your child's form tutor, head of year or a member of the safeguarding team as soon as possible.
Your or your child have a concern about online actions or behaviour which does not involve pupils from the school (e.g. cyber bullying, requesting/sharing inappropriate content, etc)	We recommend you contact the Police and discuss the concerns with them directly. The school will of course support with referring this to our assigned Police Officer if we are notified of any such concern.
Your or your child have a concern about content which is available via an online platform they are using (e.g. Age inappropriate advertising, discriminatory content, etc)	We recommend you report this to the provider and/or CEOP using the "Report It" function provided through the platform or CEOP website.
Your or your child have a ***serious*** concern about online actions or behaviour from any other people (e.g. Immanent threats, grooming, extremist materials, etc)	We recommend you contact the Police or CEOP immediately to raise your concerns.

Sources of Further Support

A wealth of information and advice is available to access online. The following websites are known nationally for providing high quality, impartial information which covers a wide range of issues of interest to parents:

NSPCC Net Aware	**Website**: www.net-aware.org.uk The NSPCC offer a wide range of resources to support children, young adults and parents to understand the key issues associated with safe and responsible use of ICT and the internet. NetAware is a particularly useful feature for parents which provide access to details about the intended use, features and safety ratings for almost all apps and websites that are available to children or young people.
CEOP A National Crime Agency command	**Website**: www.ceop.police.uk CEOP (Child Exploitation and Online Protection Command) is a partnership involving the Police, charities and industry leaders and was set up to provide support, advice and information to young people and parents. The resources and reporting tools within the website are particularly useful if things go wrong or if you want to find out about recent concerns which have been reported across the UK.
UK Safer Internet Centre	**Website**: www.saferinternet.org.uk The Safer Internet Centre offer a wide range of resources to support children, young adults and parents to understand the key issues associated with safe and responsible use of ICT and the internet. Resources are available to support all levels of prior understanding and abilities.
internet matters	**Website**: www.internetmatters.org Internet Matters offer a wide range of resources to support children, young adults and parents to understand the key issues associated with safe and responsible use of ICT and the internet. Resources are available to support all levels of prior understanding and abilities.

Appendix 5: E-Safety and the Virtual Curriculum

The closure of school in March 2020 as part of the Government's response to managing the Covid-19 outbreak has drastically changed the way that pupils interact with each other and the method Frederick Bremer provides pupils with access to educational resources. As such, specific guidance is provided within in our in our ' Child Protection and Safeguarding: COVID-19 Addendum to Safeguarding Policy - April 2020'. A summary of this guidance is provided below for easy reference but further information can be found in the full addendum.

Online safety

In school

We will continue to have appropriate filtering and monitoring systems in place in school.

If our regular in-house IT staff are unavailable, our contingency plan is to contact the IT support company Joskos directly.

Outside school

Where staff are interacting with children online, they will continue to follow our existing code of conduct and IT acceptable use policy. All communication with pupils will take place within google suite. Staff will not be doing 'live' lessons nor any visual communication with pupils or their families.

We will be sharing advice and guidance on online safety for parents and pupils in our weekly parental briefings

Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our reporting procedures as set out in section 4 of this addendum.

We will make sure children know how to report any concerns they have back to our school, and signpost them to other sources of support too.

Working with parents and carers

We will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online
- Know what our school is asking children to do online, including what sites they will be using and who they will be interacting with from our school
- Are aware that they should only use reputable online companies or tutors if they wish to supplement the remote teaching and resources our school provides
- Know where else they can go for support to keep their children safe online - this can be found at https://www.bremer.org.uk/e-safety/

What to do in different scenarios

If teachers are uploading resources to an open Google Drive

Make sure there's nothing that can identify pupils in the resources, like their names or comments addressed specifically to them, as anyone with the link can view what's in the Drive.

If you're using Google Classroom to set work and communicate

If you allow pupils to comment, tell them they should only be talking about school work in the 'Stream' and that they could be muted (prevented from posting or commenting) for posting anything inappropriate or bullying.

Give parents the chance to opt out of their child posting in the 'Stream' too. If they opt their child out, mute them.

If teachers are recording videos to share through YouTube

They must:

- Record against a neutral background
- Avoid recording in their bedroom if they can (if that's not possible, use a neutral background)
- Dress like they would for school - no pyjamas!
- Double check what other tabs they have open in their browser, if they're sharing their screen (e.g. no search results for adult content open in another tab)
- Use professional language

If they have a personal account where they've created playlists, they should set up a separate work account.

Staff should:

- Set their videos to 'Unlisted' so that only people who have the link (e.g. parents who you've emailed) will be able to see the video
- Set the audience as 'Made for kids', so that adverts won't appear at the start of the video, and comments will be disabled

If you're using Google Hangouts Meet

Although the school will not be using this for classes or individual pupils, it could potentially provide a useful platform for maintaining contact with the pupil leadership team for example.

As with recording video clips for learning staff must:

- Sit against a neutral background
- Avoid recording in their bedroom where possible (if that's not possible, use a neutral background)
- Dress like they would for school - no pyjamas!
- Double check what other tabs they have open in their browser, if they're sharing their screen (e.g. no search results for adult content open in another tab)
- Use professional language
- Ask pupils to also be in a shared space in their house, rather than in their bedroom. No pyjamas for pupils either! Alternatively, you could ask them to turn their cameras off
- Ask parents who'll also be there to be mindful of the fact that other children might see or hear them and what's in the background
- Make a recording so there's something to go back to later on if you need to, and keep a log of who's doing hangouts and when. Check that parents are happy with you making recordings first - tell them it's for school records only