E-safety Policy

November 2021

Signed …… Chair of Governors

Signed …… Headteacher

Date ……

Review date……..

Contents

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Freeland CE Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties.

The newly updated Keeping Children Safe in Education (2021) highlights the importance of e-safety in schools.

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, ipads, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised school staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the School Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's E-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner who is the headteacher. Pupil incident concerns must be passed on immediately (if serious) to a member of SLT. Bullying or racist incidents must be passed onto Designated Safeguarding Lead immediately and logged appropriately.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your School ICT support.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette;'netiquette'. The Computing Curriculum states that children should use and be familiar with email.

Managing mail

- The school gives all staff their own e-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as any letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or member of SLT.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All pupils will have their own individual school issued accounts during their time at Freeland School.

- The forwarding of chain letters is not permitted in school.

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission and virus check attachments.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

- Staff must inform the Designated Safeguarding Lead if they receive an offensive e-mail.

- Pupils are introduced to e-mail as part of the Computing Curriculum.

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending emails

- Use your own school e-mail account so that you are clearly identified as the originator of a message and when necessary copy in a member of SLT e.g. if communicating with parents.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- School e-mail is not to be used for personal advertising.

Receiving emails

- Check your e-mail regularly (ideally at least every week day, during term time)

- Activate your 'out-of-office' notification when away for extended periods.

- Never open attachments from an untrusted source.

Do not use e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where

possible.

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted. Teachers and teaching staff must only use the prescribed Outlook email addresses. Children have access to their own gmail accounts linked to their Google accounts. The activity within these email accounts is closely monitored.

- Teachers and teaching staff have access to Class Dojo/Google Classroom where they can post messages to the whole class. No sensitive information is to be posted in these domains. All protocol relating to email safety is to be adhered to when sending class Dojo/Google Classroom messages.

- Teachers and teaching are not to use this domain to directly contact parents/guardians/children outside of school. If a parent/guardian wants to talk to a member of school teaching staff they must not use these domains to contact staff. Any communication must go through the office email to protect all parties against unwanted contact.

- Both Class Dojo and Google Classroom are closely monitored by Designated Safeguarding Lead to ensure safe practice is being upheld.

- Where your conclusion is that e-mail must be used to transmit such data:

  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

  - All emails sent from staff will contain the following disclaimer:

Disclaimer: The information in this e-mail, together with any attachments, is confidential. If you have received this message in error you must not print off, copy, use or disclose the contents. The information may be covered by legal and/or professional privilege. Please delete from your system and inform the sender of the error. As an e-mail can be an informal method of communication, the views expressed may be personal to the sender and should not be taken as necessarily representing the views of Freeland CE Primary School.

As e-mails are transmitted over a public network Freeland CE Primary School cannot accept any responsibility for the accuracy or completeness of this message. It is your responsibility to carry out all necessary virus checks.

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Google Classroom in GSuite for Education

We use G Suite for Education - a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. Pupils will use their G Suite accounts to complete assignments, communicate with their teachers and learn 21st century digital citizenship skills, using mostly Google Classroom.

We use a special version of the core G Suite Apps to provide a secure learning intranet for our pupils and staff.

Children use a Gmail login to access our system servers and the intranet and internet in school. With school Gmail and Google Docs, for example, work and emails cannot be shared with external email accounts, only with others within @freelandprimary.co.uk - the school's Google domain. Google requires basic information to set up these accounts, your child's leaving year and name.

Google Cloud does contain much of the electronic work that your child completes in school. By logging in at home, using the same login as at school, your child can continue working on projects started in school, often using one of the main apps of G Suite, Google Classroom.

Our pupil accounts have a particular set of security settings to reflect the fact that the system is being used by a child - they have a much higher security setting than our staff for example. We take advice on these settings from companies that advise us.

On leaving the school, we can transfer your child's digital learning record to his/her own gmail account through the Google TakeOut system - the school does not then retain any data. This can be a wonderful souvenir of learning. Google accounts are deleted within a few weeks of a child leaving Freeland Primary School.

Google's Privacy Policy for GSuite can be found here:

https://policies.google.com/privacy/update

The information below from Google provides answers to common questions about what they can and can't do with your child's personal information, including:

What personal information does Google collect?

How does Google use this information?

Will Google disclose my child's personal information?

Does Google use student personal information for users in K-12 schools to target advertising?

Can my child share information with others using the G Suite for Education account?

G Suite for Education information for Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from pupils in connection with these accounts.

Using their G Suite for Education accounts, pupils may access and use the following "Core Services" offered by Google Classroom

(described at https://gsuite.google.com/terms/user_features.html):

Gmail

Calendar

Docs

Sheets

Slides

Forms

Drive

Sites

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html

You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a pupil account, we provide Google with certain personal information about our pupils, including, for example, a name, email address, and password. Google may also collect a profile photo added to the G Suite for Education account, but the school will not support the upload of personal photos of children.

When a pupil uses Google services, Google also collects information based on the use of those services. This includes:

device information, such as the hardware model, operating system version, unique device

identifiers, and mobile network information including phone number;

log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;

location information, as determined by various technologies including IP address, GPS, and other sensors;

unique application numbers, such as application version number; and

cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

Does Google use student personal information for users in primary schools to target advertising?

No. For G Suite for Education users in primary and secondary schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

We allow pupils to access Google services such as Google Docs and Sites, which include features where users can share information with others within our Internet domain here at Freeland.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organisations and individuals outside of Google unless one of the following circumstances applies:

With parental or guardian consent. Google will share personal information with companies, organisations or individuals outside of Google when it has parents' consent which may be obtained through G Suite for Education schools - including Freeland. We would contact parents directly if Google asks for any examples of children's work etc.

With Freeland School G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.

For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.

For legal reasons. Google will share personal information with companies, organisations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

meet any applicable law, regulation, legal process or enforceable governmental request.

enforce applicable Terms of Service, including investigation of potential violations.

detect, prevent, or otherwise address fraud, security or technical issues.

protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

- Where your conclusion is that e-mail must be used to transmit such data:

  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

  - All emails sent from staff will contain the following disclaimer:

    Disclaimer: The information in this e-mail, together with any attachments, is confidential. If you have received this message in error you must not print off, copy, use or disclose the contents. The information may be covered by legal and/or professional privilege. Please delete from your system and inform the sender of the error. As an e-mail can be an informal method of communication, the views expressed may be personal to the sender and should not be taken as necessarily representing the views of Freeland CE Primary School.

    As e-mails are transmitted over a public network Freeland CE Primary School cannot accept any responsibility for the accuracy or completeness of this message. It is your responsibility to carry out all necessary virus checks.

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Pupils with Additional Needs

Staff are aware that some pupils may require additional support including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has limited social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

E safety – Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety coordinators in this school are Mrs P McCarthy and Mr J Lambert. The named e-safety coordinator governor is Mr N Dawson. All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet..

SLT and Governors are kept updated and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

E Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and regularly referred to.

- The school has a framework for teaching internet skills in ICT lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise as well as part of the e-safety curriculum
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through

cross curricular teacher models, discussions and via the Computing curriculum.

E Safety Skills development for staff

- Our staff receive updates and training on e-safety issues from the Computing Subject Leader.
- New staff are given information and sign the school's acceptable use policy.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Misuse and Infringements

Complaints

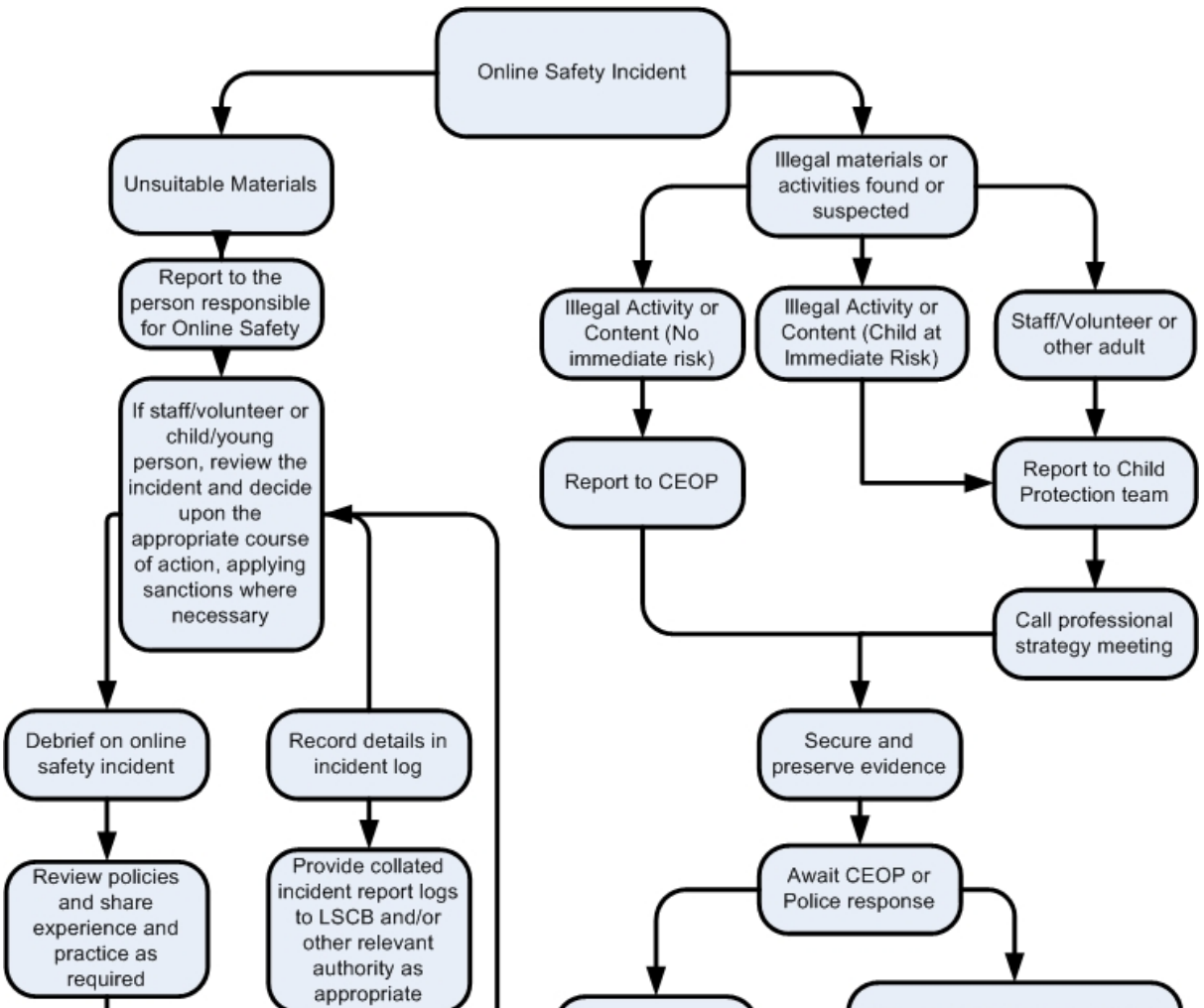
Complaints and/ or issues relating to e-safety should be made to the e-safety co-ordinator or head teacher. Incidents should be logged and the **Flowcharts for Managing an e-safety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the head teacher/, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Freeland CE Primary School

Flowcharts for Managing an E Safety Incident



Freeland CE Primary School

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group/Class:
Date:
Reason for investigation:

Details of first reviewing person
Name:
Position:
Signature:

Details of second reviewing person
Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken	

Internet Access

Managing the Internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- All users must observe copyright at all times.

Internet Use

- Do not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended audience.
- Do not reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- On-line gambling or gaming is not allowed in school or on school ICT resources.

It is at Designated Safeguarding Lead's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Freeland CE Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; the EY General Data Protection Regulation (GDPR), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given a safety check first.
- Pupils are not permitted to download programs or files on school based technologies without seeking prior permission from the head teacher.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Social Networking Sites

- At present, the school endeavors to deny access to social networking sites to pupils within school

- We encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests).

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

- Our pupils are asked to report any incidents of bullying to the school.

- Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy.

- The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

- If an allegation of bullying does come up, the school will:

  • take it seriously

  • act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully

  • record and report the incident

  • provide support and reassurance to the victim

  • make it clear to the ‘bully’ that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group

- It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

- If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website)
- Parents/ carers are asked to sign a statement agreeing to follow the e-safety rules. (see Appendix 2)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items

Passwords

- Always use your own personal passwords to access computer based services.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary,

and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

- Passwords must contain a minimum of six characters and be difficult to guess.
- User ID and passwords for staff and pupils who have left the School are removed from the system within one week.

If you think your password may have been compromised or someone else has become aware of your password report this to Designated Safeguarding Lead.

Passwords Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. We are also aware that
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations/laptops/ipads are locked if left unattended.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of Designated Safeguarding Lead, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff

device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

- If pupils bring a mobile phone or similar device into school, it should be handed into the office at the start of the day and returned to the owner at home time.

Publishing pupils images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site or Learning Platform.

- In the school prospectus and other printed publications that the school may produce for promotional purposes

- Recorded/ transmitted on a video or webcam

- In display material that may be used in the school's communal areas

- In display material that may be used in external areas, i.e. exhibition promoting the school

- General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' surnames will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.
Only Staff members and the Web Manager has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Designated Safeguarding Lead.

- Staff must use password protected USB sticks if they wish to store / transfer images.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.

- The administrator has the responsibility of deleting the images when they are no longer required.

Videoing and Conferencing

- IRIS connect is a learning tool used to support teacher learning. It involves videoing the teacher, small groups or the whole class and then watching the video back to gain insight, teacher targets etc.

- Teachers will only use the videos for professional purposes.
- Teachers will only share the videos with other members of the school teaching staff and if appropriate the class or group who have been videoed.

Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on

the school's network drive.

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network without prior consent of the headteacher/ICT manager
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical

Portable & Mobile ICT Equipment

This section covers such items as laptops, ipads, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop / ipad in the boot of your car before starting your journey.
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the computing subject leaders, fully licensed and only carried out by your ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move

towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that they are used appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. These must be kept in cupboards in classrooms. If a mobile phone is to be used it must be in child free areas e.g. the staff room or office. Only in exceptional circumstances should a member of staff contact a pupil or parent/carer using their personal device.

- Under no circumstances should staff use their mobile phone during learning time or in areas that pupils have access to.

- Pupils are not allowed to bring personal mobile devices/phones to school unless permission has been given by Parents and Staff members. If they are brought in as a safety feature e.g. the child is walking home alone, the phone will be handed into the office at the start of the day and returned at home time.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any members of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Writing and Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the E-safety coordinator any issue of e-safety that concerns them.
There will be an on-going opportunity for staff to discuss with Designated Safeguarding Lead any issue of data security that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors on……

The implementation of this Policy will be monitored by Designated Safeguarding Lead.

Current Legislation

Acts Relating to Monitoring of Staff email

The EU General Data Protection Regulation (GDPR)

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. It expands the rights of individuals to control how their personal data is collected and processed.

Paper cut has been installed on the staff room printer to ensure that sensitive information is only read by those intended to read it.

Any GDPR data breach needs to be reported immediately to the GDPR officer (Joe Lambert/Colin Plaice) to be investigated further.

For further information on GDPR please see the EPA GDPR policy.

https://www.epa-mat.org/gdpr-policies/

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Human Rights Act 1998

Other Acts Relating to eSafety

Teaching Children Safely Online 2020

This outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It complements existing and forthcoming subjects including Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing. It does not imply additional content or teaching requirements.

It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils. Schools can refer to the Education for a

Connected World Framework for age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Education for a Connected World 2020

Education for a Connected World is a tool for anyone who works with children and young people. It enables the development of teaching and learning as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world. It focuses specifically on eight different aspects of online education:

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of the "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other to fear on each of those occasions

*The following user agreement policies are to go out at the start of every school year/when a new child, teaching staff member or governor has started.

Key Stage One Pupil Acceptable Use

Agreement / eSafety Rules

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): _____

Signed (parent): _____

Key Stage Two Pupil Acceptable Use

Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details, such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer may be contacted if a member of school staff is concerned about my e-safety.

Signed ……..Date…….

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc is an integral important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these e-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like to discuss this further please contact Designated Safeguarding Lead.

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details, such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer may be contacted if a member of school staff is concerned about my e-safety.

✂----------

Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the e-safety rules and to support the safe use of ICT at Freeland CE Primary .

Parent/ Carer Signature ……

Class …… Date ……

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the Designated Safeguarding Lead.

I will only use the school's email, Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities

I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.

I will only use the approved, secure e-mail system(s) for any school business.

I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.

I will not install any hardware or software without permission of the Computing Leaders/HeadTeacher.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff

member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or the Head teacher.

I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

I will not use my own personal device to take and upload photos of children in school

I understand that all my use of the Internet and other related systems can be monitored and logged and can be made available, on request, to my line manager or Head teacher.

I will respect copyright and intellectual property rights.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute, this includes my use of any social media.

I will support and promote the school's e-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…….……. Date

……

Full Name ……..……..(printed)

Job title . . . . . .