FARNEY CLOSE SCHOOL

E Safety Policy

<u>The Review Date of this policy has been changed to bring it in line with yearly KCSiE updates</u>

Date Published	January 2022
Reviewed	September 2023
Next Review Due	September 2024
Author	John Pelling

Approval Level	☑ Governing Body □ Principal to Determine
Signed	
Role	Governor
Date Approved	

CONTENTS

1. Aims

Farney Close School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given school staff stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

This policy applies to all members of the school community including all staff, pupils, or any other person given access to the school's IT systems, both inside and outside of the school.

3.1 The Governing Body

The Governing Board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Governor who oversees online safety is Carole Johns.

All Governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

3.2 The Principal

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

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputy/Deputies are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the Principal, ICT Manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Facilitating regular, planned staff training on online safety issues including awareness training on child exploitation, radicalisation and cyber-bullying.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and/or Governing Board.

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure (including ensuring that passwords and security prevent unauthorised access) and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Delivering (or organising the delivery of) an approved e-safety training program as part of all staff induction.
- Delivering (or organising the delivery of) e-safety training for individual staff as identified during any supervision, appraisal or other professional meeting.
- Conducting a full security check and monitoring the school's ICT systems on a termly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently across the whole curriculum and other activities.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Undertaking training to ensure their knowledge allows them to fulfil their professional responsibilities.

This list is not intended to be exhaustive.

3.6 Pupils

Pupils are responsible for:

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet.
- Uunderstanding the importance of reporting abuse, misuse or access to inappropriate materials to members of staff whenever it might occur.
- Handing in all mobile devices, digital cameras / video recorders / sound recorders, internet tablets, laptops, or any other similar device when they return to school.
- Knowing and understanding the dangers of taking or sharing images and of cyber-bullying.
- Understanding the importance of adopting good e-safety practice when using digital technologies outside of school.
- Realising that the school's e-safety policy covers their actions out of school if it is related to their membership of the school.
- Recognising that the school will communicate with their parents/carers or any other agency if it believes that their actions place themselves or anyone else at risk.
- Have a good understanding of why they should avoid plagiarism and uphold copyright regulations.

This list is not intended to be exhaustive.

3.7 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- Support the school in keeping all pupils safe online including sharing information and the searching of personal devices as detailed in section 6.3
- Not take photographs or videos of any pupil other than their own, or a pupil they have parental responsibility for, whilst at school or during any school connected activity.
- Understand they can ask for support, information and guidance from the school on e-safety at any time.

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

What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the 24-hour curriculum; that is during both educational and social times. The e-safety curriculum in school time will be broad, relevant and provide progression with opportunities for creative activities and discussion. There are a number of events throughout the year that also encompass e-safety including anti-bullying week and talks from external speakers.

e-safety education may be provided in the following ways:

- A planned e-safety curriculum will form part of IT and PHSE lessons and will be regularly revisited.
- The safe use of technology, social media and the internet will also be covered in other subjects where relevant.
- Education staff will also ensure that e-safety messages and guidance are included in all lessons as and when appropriate.
- Key e-safety messages should be reinforced as part of a planned programme of educational, pastoral or social development activities, including evening activities.
- Pupils will be encouraged and supported in responding to and participating in national events that focus on e-safety.
- In all lessons, all pupils should be taught to be critically aware of the materials and content they access online.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- All classrooms and houses will have an e-safety booklet available for pupils and staff will be uses as an advisory reference.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Every residential unit has a copy of the schools Anti-Bullying leaflet. The school also provides information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying Policy and Procedure. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

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

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

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

8. Pupils using mobile devices in school

Unless an agreement is in place, pupils must give in all mobile devices, digital cameras / video recorders / sound recorders, internet tablets, laptops, or any other similar device when they return to school. Where an agreement is made, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger appropriate sanctions in line with the school behaviour policy, which may result in the confiscation of their device.

9. Anyone using work devices outside school

Anyone using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Everyone must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If anyone has any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

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

11. Training

During staff induction, where possible between being appointed and starting work, staff are allocated induction sessions with the IT support team. This enables IT support staff to set up the appropriate accounts, provide an overview of e-safety systems and procedures and make sure that the staff member is confident in relation to e-safety. These sessions include details of the benefits and limitations of our e-safety systems so that realistic expectations are set from the start.

All new staff members will receive training on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

As a side note, a basic IT assessment is undertaken as well as asking the new staff member if there are any health and safety or support related considerations to using IT; for example, if they suffer from migraines, eye-sight issues or dyslexia etc. Where appropriate, this is used to schedule further IT training and support sessions with IT Support staff or external companies.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The IT Support staff attend external training to ensure that their knowledge is up-to-date. In addition, the school has supported this team in networking with other schools. This enables two-way information and knowledge sharing. The school has contact with the regional specialist e-safety police team within the South East Regional Organised Crime Unit (SEROCU) and a specialist cyber security company called InfoSec. We also rely on information from government websites including the National Cyber Security Centre and have gained advice from the National Crime Agency.

The DSL and Deputy/Deputies will undertake Child Protection and Safeguarding Training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Risk Assessing pupils e-safety

12.1 Preventing and addressing e-safety risks

Where there is an incident which presents a significant risk or concern immediate action should be taken to stop the risk continuing either directly or by calling for a member of the IT Support team to intervene. This should be done as discreetly as possible and the response should reflect the seriousness (or otherwise) of the incident. An e-safety reporting form should be completed as soon as possible. The Network Manager will take responsibility for sharing this information with the SLT/DSL as appropriate.

If the staff member does not feel it is appropriate to share this information with the IT Support team they should request that a pupil's internet/network access is blocked and explain the issue itself is being dealt with by the SLT or DSL. In this instance, the member of staff should complete an e-Safety Reporting Form but hand it to the SLT/DSL. They will involve the IT Support team as they see fit.

If e-safety information comes in from an external source the member of staff receiving this information should complete an e-Safety Reporting Form with the relevant details and pass it to the IT Support team, SLT or DSL as detailed above. The IT Support team will maintain a spreadsheet of concerns to enable any patterns or concerns to be identified and shared appropriately with others.

The IT Support team receive notifications of web filter violations and when any IT user triggers a key word/phrase alert. If they receive this information, they will take immediate and appropriate action to resolve the situation and inform the staff of their concerns. They can remotely monitor staff and pupil PC's/Laptops and act if required.

12.2 Determining a Pupil's level of risk

There is no definite answer to determining a pupil's level of risk. However, as an indication each pupil is categorised as a high, medium or low risk in relation to e-safety.

High Risk is usually an indication that a pupil has repeatedly attempted to access content identified by the security systems (or staff) as adult/mature content, potentially liable or security risk categories. It can also be attributed to pupils who repeatedly attempt to get around security measures to either access information they shouldn't or cause harm to the systems or others.

Medium Risk is usually an indication that a pupil has repeatedly attempted to access content of concern (not in the above categories) or has behaved in a way that has attempted to disrupt learning or use of IT. For example, repeatedly attempting to use 'hacking' software or access social media sites or anonymous search engines.

Low Risk is usually an indication that there are little or no concerns in relation the pupil.

Risks can relate to any e-safety related incident whether it occurred inside or outside of the school.

A pupil's risk assessment in relation to e-safety is reviewed and updated whenever necessary to ensure its accuracy. The Network Manager responsible for ensuring that this aspect of the pupil's risk assessment is kept up-to-date and accurate. (S)he is responsible for alerting the SLT, DSL and other staff of any significant changes and where appropriate gaining permission to add such information to the risk assessment.

12.3 Implications of each pupil's risk level

Depending on the determined risk level of an individual the following procedures will be put in place:

High Risk pupils have their browsing history and document folders checked once a week and all websites are checked where there is a concern.

Medium Risk pupils have their browsing history and document folders checked every 5 weeks; three weeks browsing history is checked out of every 5-week cycle.

Low Risk pupils have their browsing history and document folders checked every 8 weeks; three weeks browsing history is checked out of every 5-week cycle.

In addition, key word / phrase checking software results are reviewed once a week for <u>all</u> Pupils irrespective of risk level. This monitors for phrases associated with suicide, radicalisation, drugs, bullying and other categories of concern.

13. Monitoring arrangements

There are many ways in which we monitor and evaluate the effectiveness of our e-safety systems including:

- keeping records of risk level of individuals through the pupil's risk assessment
- Keeping records of all e-safety reports to establish if the number of reports has gone down, stayed the same or risen.
- Keeping records of all e-safety information in order to establish any patterns of concerning behaviour.
- Keeping records of all staff, pupil and other user web history, keyword history and document searches.
- Reviewing a weekly whole site web activity report. This enables us to identify any significant concerns. For example, it shows the top websites visited and blocked by user and volume, browse

time, most blocked users etc. Whilst not necessarily useful in itself, it can lead us to investigate any concerns about the system in general and individually identified users.
- Reviewing a weekly whole site cyber threat assessment report. This enables us to quickly see any causes for concern in terms of the security of our network including servers and PC's.

It is very difficult to extract statistical data for the purposes of evaluating the effectiveness of our e-safety systems over time. There is too much contextual information required to make such a determination for it to be accurate. For example, a pupil may have a lower number of incidents due to an internet ban. However, our monitoring and evaluation procedures do enable us to identify and act upon incidents and patterns of concerning behaviour.

The SLT/DSL log behaviour and safeguarding issues related to online safety including (where appropriate) actions taken.

This policy will be reviewed bi-annually by the Network Administrator. At every review, the policy will be shared with the governing board.

14. Links with other policies

This online safety policy is linked to our:

IT Business Continuity Plan

Cyber Attack and Data Breach Policy

Safeguarding and Child Protection Policy

Behaviour Policy

Staff Disciplinary Procedures

Data Protection Policy and Privacy Notices

Farney Close School
Acceptable Use Agreement – Pupils

When using the school's ICT systems and accessing the internet, I will not:

- Use them for a non-educational purpose
- Use them without a responsible adult being present or without a member of staff's permission
- Access or attempt to access, create or share any inappropriate or illegal content. This includes downloading or accessing anything that is copyright protected
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity or permission has been given from a member of staff)
- Use chat rooms or social messaging systems
- Open any attachments or follow any links in emails, without first checking with a member of staff
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Use a password that is used outside of school or elsewhere
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Do anything to try and get around the school's IT security systems including web filters
- Install or attempt to install any software without prior consent from the Principal and/or IT Support

If I bring a personal mobile phone(s) or other personal electronic device(s) into school:

- I will hand all devices in when on on-site, on school activities or when requested by a member of staff
- I will not use them at any time without first getting permission from a member of staff
- I will use them responsibly, and will not access or attempt to access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- If the principal or safeguarding person are concerned about anything stored on a personal device(s), they have the right to tell my parents/carers, police, social services and/or delete any content they feel is inappropriate

I agree that the school will monitor the websites I visit and what I am doing whilst using the school's ICT systems and internet including internet usage on my own devices when connected to the school systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly.

Pupil Name		**Date:**
Signed (Pupil):		
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff or responsible adult. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.		
Signed (Parent/Carer):		**Date:**

Farney Close School
Acceptable Use Agreement –
Staff, Governors, Volunteers & Visitors

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access or attempt to access, create or share any inappropriate or illegal content including but not limited to material of a violent, criminal or pornographic nature. This includes downloading or accessing anything that is copyright protected
- Access social networking sites, chat rooms or social messaging systems except when permitted to do so by the principal
- Use them in any way which could harm the school's reputation
- Open any attachments in emails, or follow any links in emails if I have concerns about their legitimacy and safety
- Use any inappropriate language when communicating online, including in emails or other messaging services
- Share my password with others or log in to the school's network using someone else's details
- Use a password that is used outside of school or elsewhere
- Do anything to try and get around the school's IT security systems including web filters
- Install or attempt to install any software without prior consent from the Principal and/or the IT Support team

When using the school's internet connection on personal devices:

- I will not disclose the wireless access password to any other person including colleagues
- I will always keep my personal devices in a secure place and must not allow anyone else to use or access my personal devices
- I will not use personal devices whilst working with, responsible for or in the vicinity of pupils with the exception of a sleeping in duty so long as the pupils are asleep. If I need to maintain essential/emergency contact via a mobile phone whilst at work, I must first seek permission from the Principal, Head of Education or Care Manager.

All applicable terms and conditions detailed anywhere within this policy also apply when using personal devices

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and what I am doing whilst using the school's ICT systems and internet including internet usage on my own devices when connected to the school 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.

By signing below, I agree to abide by the terms and conditions set out in this policy. Failure to do so may result in my personal device access being withdrawn and/or disciplinary/other action being taken against me in line with school policies.

Name		**Date:**
Signed (Staff Member, Governor, Volunteer or Visitor):		

E Safety Pupil Incident Log

Incident Number	Date	Name	Reported by (Initials)	Reported to (Initials)	Checked by Governor (Initials)

E Safety Staff Incident Log

Incident Number	Date	Name	Reported by (Initials)	Reported to (Initials)	Checked by Governor (Initials)

Farney Close School
E-Safety Reporting Template

Incident Number	Name of Person(s) Involved	Incident Date	Incident Time	Location	Incident Report By	Incident Reported To

What Happened?
What Action Was Taken? By Who?

Staff Name		**Manager Name**	
Signature		**Manager Signature**	

Farney Close School
Loan Equipment Agreement - Staff

ICT Equipment is loaned to you by Farney Close School (hereafter known as the school) on a temporary basis in order to help with the preparation of your teaching and learning resources, meet your professional responsibilities and to help with access to online resources when inside the school or at home.

1. The loan agreement exists between the school and the named person who has signed this loan agreement.

2. ICT equipment will be loaned to the named person for an agreed period of time during their employment and must be returned if the employment ceases, or at any time if requested by the ICT tech team for the purposes of maintenance (point 8 below) or by any member of the SLT.

3. All loaned equipment and associated peripherals remain the property of the school.

4. All loaned equipment will come with any required software pre-installed. If you have any technical issues with the equipment, this should be reported to the ICT tech team at the earliest opportunity. An ICT technician must carry out all software installations.

5. At no point must you attempt to make any changes or repairs to the loan equipment hardware. Any hardware repairs or upgrades must be done by the ICT tech team.

6. The computer and the connectivity equipment must not be used for any illegal and/or anti-social purpose and must be used in accordance with the Staff Acceptable Use Agreement and e-safety policy.

7.All activity on loan equipment, both online and offline, may be monitored by the school wherever this activity takes place. You will responsible for any activity on loan equipment and should a breach of the Staff Acceptable Use Agreement be discovered action will be taken in accordance with school policies.

8. There may be occasions when we need you to return the computer to school for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the computer. Farney Close cannot be held responsible for the loss or damage of any data on the computer during this process. It is your responsibility to ensure that you have backed up any data you wish to keep and to return the equipment to school when requested.

9. Personal data should not be stored on any school owned equipment.

10. If any equipment is stolen you must immediately report it to the police and get a crime reference number, and immediately report this to SLT and the ICT tech team.

11. In the event of any equipment being stolen or accidentally damaged, we will do our best to repair or replace it. Please note that it is not always possible to repair or replace equipment immediately.

Responsibilities you have to care for loaned equipment:

12. You have a responsibility to take reasonable care to ensure the safety and security of the loan equipment and any data stored, accessible via or accessed on it.

13. You have a responsibility to use the loan equipment in accordance with school policies and agreements relating (but not limited) to e-safety, data protection, health and safety and acceptable use.

13. You must not remove any labels that are attached to the equipment, including but not limited to, asset labels and PAT testing labels.

14. Reasonable health and safety precautions should be taken when using ICT Equipment. The school is not responsible for any damage to person or property resulting from the misuse of equipment.

This agreement applies to any equipment loaned to staff including (but not limited to) the following:

Equipment Type & Brand	Name / Serial No.	Date Issued	Duration	Return Date

Please sign below to acknowledge you have read (or had explained) and understand the terms and conditions in the loan agreement and agree to abide by them.

Staff Name		**Manager Name**	
Signature		**Manager Signature**	
Date		**Date**	

Farney Close Loan Equipment Agreement – Staff. 4th January 2019

Farney Close School
Loan Equipment Agreement - Pupils

Farney Close School (hereafter known as the school) may provide you with a laptop or other equipment on a temporary basis. This is to support you with your learning and to enable you to access online resources when inside the school or at home.

1. This loan agreement exists between the school and the named pupil who has signed this loan agreement.

2. ICT equipment will be loaned to the named pupil for an agreed period of time and must be returned at the end of your education at the school, or at any time if requested by the ICT tech team for the purposes of maintenance (point 9 below) or by any member of the SLT.

3. If the laptop has been purchased for the named pupil then, when a pupil ends their education at the school, the ICT tech team will (upon request) restore the laptop to its original settings so that it can be used without restriction.

4. Unless you have been told that the laptop (or other equipment) you are using has been provided by anyone other than the school (e.g. by your local authority) then the equipment and associated peripherals remain the property of the school. You must still agree to the conditions of this agreement and the Pupil Acceptable Usage Agreement when using any equipment.

5. All loaned equipment will come with any required software pre-installed. If you have any technical issues with the equipment, this should be reported to the ICT tech team at the earliest opportunity. An ICT technician must carry out all software installations.

6. At no point must you attempt to make any changes or repairs to the loan equipment hardware. Any hardware repairs or upgrades must be done by the ICT tech team.

7. The computer and the connectivity equipment must not be used for any illegal and/or anti-social purpose and must be used in accordance with the Pupil Acceptable Use Agreement.

8.All activity on loan equipment, both online and offline, may be monitored by the school wherever this activity takes place. You will responsible for any activity on loan equipment and should a breach of the Pupil Acceptable Use Agreement be discovered action will be taken in accordance with school policies.

9. There may be occasions when we need you to return the computer to school for upgrades and maintenance. Please note that because of these upgrades, it may be

necessary to completely remove all information contained on the computer. Farney Close cannot be held responsible for the loss or damage of any data on the computer during this process. It is your responsibility to ensure that you have backed up any data you wish to keep and to return the equipment to school when requested.

10. Personal data should not be stored on any school owned equipment.

11. If any equipment is stolen you must immediately report it to the police and get a crime reference number, and immediately report this to SLT and the ICT tech team.

12. In the event of any equipment being stolen or accidentally damaged, we will do our best to repair or replace it. Please note that it is not always possible to repair or replace equipment immediately.

Responsibilities you have to care for loaned equipment:

13. You have a responsibility to take reasonable care to ensure the safety and security of the loan equipment and any data stored, accessible via or accessed on it.

14. You have a responsibility to use the loan equipment in accordance with school policies and agreements relating (but not limited) to e-safety, data protection, health and safety and acceptable use.

15. You must not remove any labels that are attached to the equipment, including but not limited to, asset labels and PAT testing labels.

16. Reasonable health and safety precautions should be taken when using ICT Equipment. The school is not responsible for any damage to person or property resulting from the misuse of equipment.

This agreement applies to <u>any</u> equipment loaned to pupils including (but not limited to) the following:

Equipment Type & Brand	Name / Serial No.	Date Issued	Duration	Return Date

Please sign below to acknowledge you have read (or had explained) and understand the terms and conditions in the loan agreement and agree to abide by them.

Pupil Name		**Manager Name**	
Signature		**Manager Signature**	
Date		**Date**	

Farney Close School
Web Filtering Arrangements

We currently use a Fortigate Web Filter / Firewall to protect our network and users. This document details the categories of web filtering and whether they are monitored or blocked for users by default. We also have the ability to allow or block individual websites as deemed appropriate by the SLT.

Websites

Category / Description	Pupil in Hours	Pupil out of Hours	Staff	BYOD
Adult / Mature Content				
Abortion	✗	✗	✗	✗
Advocacy Organizations	✗	✗	✗	✗
Alcohol	✗	✗	✗	✗
Alternative Beliefs	✗	✗	✗	✗
Dating	✗	✗	✗	✗
Gambling	✗	✗	✗	✗
Lingerie and Swimsuit	✗	✗	✗	✗
Marijuana	✗	✗	✗	✗
Nudity and Risque	✗	✗	✗	✗
Other Adult Materials	✗	✗	✗	✗
Pornography	✗	✗	✗	✗
Sex Education	✗	✗	✓	✓
Sports Hunting and War Games	✗	✗	✗	✗
Tobacco	✗	✗	✗	✗
Weapons (Sales)	✗	✗	✗	✗
Potentially Liable				
Child Abuse	✗	✗	✗	✗
Discrimination	✗	✗	✗	✗
Drug Abuse	✗	✗	✗	✗
Explicit Violence	✗	✗	✗	✗
Extremist Groups	✗	✗	✗	✗
Hacking	✗	✗	✗	✗
Illegal or Unethical	✗	✗	✗	✗
Plagiarism	✗	✗	✗	✗
Proxy Avoidance	✗	✗	✗	✗

Category / Description	Pupil in Hours	Pupil out of Hours	Staff	BYOD
Security Risk				
Dynamic DNS	✗	✗	✗	✗
Malicious Websites	✗	✗	✗	✗
Newly Observed Domain	✗	✗	✗	✗
Newly Registered Domain	✗	✗	✗	✗
Phishing	✗	✗	✗	✗
Spam URLs	✗	✗	✗	✗
General Interest - Business				
Armed Forces	✓	✗	✓	✓
Business	✓	✗	✓	✓
Charitable Organizations	✓	✗	✓	✓
Finance and Banking	✓	✗	✓	✓
General Organizations	✓	✗	✓	✓
Government and Legal Organizations	✓	✗	✓	✓
Information Technology	✓	✗	✓	✓
Information and Computer Security	✗	✗	✓	✓
Online Meeting	✗	✗	✓	✓
Remote Access	✗	✗	✓	✓
Search Engines and Portals	✓	✗	✓	✓
Secure Websites	✓	✗	✓	✓
Web Analytics	✓	✗	✓	✓
Web Hosting	✓	✗	✓	✓
Web-based Applications	✓	✗	✓	✓
General Interest - Personal				
Advertising	✓	✗	✓	✓
Arts and Culture	✓	✗	✓	✓
Auction	✗	✗	✓	✓
Brokerage and Trading	✗	✗	✓	✓
Child Education	✓	✗	✓	✓
Content Servers	✓	✗	✓	✓
Digital Postcards	✗	✗	✓	✓
Domain Parking	✓	✗	✓	✓
Dynamic Content	✗	✗	✓	✓
Education	✓	✗	✓	✓
Entertainment	✓	✗	✓	✓
Folklore	✓	✗	✓	✓
Games	✗	✗	✓	✓
Global Religion	✓	✗	✓	✓
Health and Wellness	✓	✗	✓	✓
Instant Messaging	✗	✗	✗	✗
Job Search	✓	✗	✓	✓
Meaningless Content	✗	✗	✗	✗
Medicine	✓	✗	✓	✓
News and Media	✓	✗	✓	✓

Newsgroups and Message Boards	✘	✘	✓	✓
Category / Description	Pupil in Hours	Pupil out of Hours	Staff	BYOD
Personal Privacy	✘	✘	✘	✘
Personal Vehicles	✓	✘	✓	✓
Personal Websites and Blogs	✘	✘	✓	✓
Political Organizations	✓	✘	✓	✓
Real Estate	✓	✘	✓	✓
Reference	✓	✘	✓	✓
Restaurant and Dining	✓	✘	✓	✓
Shopping	✘	✘	✓	✓
Social Networking	✘	✘	✘	✓
Society and Lifestyles	✘	✘	✓	✓
Sports	✓	✘	✓	✓
Travel	✓	✘	✓	✓
Web Chat	✘	✘	✘	✘
Web-based Email	✘	✘	✓	✓
Bandwidth Consuming				
File Sharing and Storage	✘	✘	✓	✓
Freeware and Software Downloads	✘	✘	✓	✘
Internet Radio and TV	✓	✘	✓	✓
Internet Telephony	✘	✘	✘	✘
Peer-to-peer File Sharing	✘	✘	✘	✘
Streaming Media and Download except YouTube	✘	✘	✓	✓

✓ Websites are Monitored ✘ Websites are Blocked

Fortinet's descriptions of each web filtering category can be found at:

https://fortiguard.com/webfilter/categories

Filtering Based on the Program or Application Being Used

Category / Description	Pupil in Hours	Pupil out of Hours	Staff	BYOD
Business	✓	✗	✓	✗
Email	✗	✗	✓	✗
Mobile	✗	✗	✓	✗
Proxy	✗	✗	✗	✗
Storage / Backup	✗	✗	✓	✗
VoIP / Voice Calls over Internet	✗	✗	✗	✗
Cloud.IT	✗	✗	✓	✗
Game	✗	✗	✗	✗
Network Service	✓	✗	✓	✗
Remote Access	✗	✗	✓	✗
Update	✓	✗	✓	✗
Web Client / Browser	✓	✗	✓	✗
Collaboration	✗	✗	✓	✗
General Interest	✓	✗	✓	✗
P2P / File Sharing	✗	✗	✗	✗
Social Media	✗	✗	✗	✗
Video / Audio	✓	✗	✓	✗
Unknown Applications	✗	✗	✗	✗

✓ Websites are Monitored ✗ Websites are Blocked

Fortinet's descriptions of each web filtering category can be found at:

https://fortiguard.com/appcontrol/categories

The UK Safer Internet Centre provides the following document, supplied by Fortinet, to show demonstrate how Fortinet meets the national defined 'appropriate filtering standards' as required under KCSIE.

Fortinet Appropriate Filtering for Education Settings