Abbey Court School

LOCATION: SCHOOL HANDBOOK, SECTION 2, DOCUMENT 23

E-SAFETY POLICY

"This policy should be read as part of a collection of policies that together form the overall Safeguarding Policy and procedure for Abbey Court School."

All staff employed at Abbey Court are subject to this policy.

Date policy first adopted: December 2020
Date reviewed: January 2024
Reviewed By: Lynne Barnes / Evey Charlton
Date ratified by Governing Body: n/a
Date of next review: Spring 2026

This policy covers:

1. **Social Media Networking**
2. **Internet Access/E-safety**
3. **Strategies for preventing misuse of Internet access**
4. **Sexting**
5. **Sensible use of emails/Internet/mobile phones**

Section 1 - Social Networking

1. Introduction

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our School Community and partners, our legal responsibilities and our reputation.
For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

2. Purpose

The purpose of this policy is to ensure:

- all children are safeguarded
- that Abbey Court School, its leaders and governors are not exposed to legal risks;
- that the outstanding reputation of Abbey Court School, staff and governors at the school are not adversely affected;
- that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of Abbey Court School.

3. Scope

This policy covers the use of social networking applications by School Employees and Governors and by partners or other third parties on behalf of the School.

These groups are referred to collectively as 'Staff' for the purpose of this policy.
The requirements of this policy apply to all uses of social networking applications which are used for any school or local authority related purpose regardless of whether the applications are hosted corporately or not. They must also be considered where Staff are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:
Blogs, Online discussion forums, Collaborative spaces, Media sharing services, and 'Microblogging' applications. Examples include Twitter, Facebook, Instagram, Snapchat, WhatsApp, YouTube etc.

Many of the principles of this policy also apply to other types of online presence such as virtual platforms.

All Staff should bear in mind that information they share through social networking applications, even if they are in private spaces, is still subject to Copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School and Local Authority Equality and Safeguarding Policies.

Staff must also be aware that involvement in discussion groups, blogs and social network systems (e.g. Facebook and Instagram) should be for personal interest only and not offer opinions, views or photos that could bring the reputation of the school into disrepute Linking on social media with a parent(s) of the school is discouraged unless these are family members. Any such link should be notified to the Headteacher.

Any communication received from children to Staff must be immediately reported to the Head Teacher, Designated Safeguarding Lead and procedures for safeguarding followed.

If a School Representative is made aware of any other inappropriate communications involving any child and social networking, these must be reported immediately, using the above procedures.

The school internet policy must be used at all times when children use ICT and access the internet in school (See the Computing policy).

4. Staff Training

The policy is introduced to staff during their induction and subsequently regular opportunities are scheduled in teaching staff meetings. Whole staff briefings are also used to reiterate this policy and to consider scenarios, enabling staff to appreciate the potential consequences.

5. Enforcement

Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible School representative being suspended.

The Local Authority reserves the right to require the closure of any applications or removal of content published by Staff which may adversely affect the reputation of the School or put it at risk of legal action.

Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority's Dismissal and Disciplinary Policies apply. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

Abbey Court Community School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Section 2 - Internet Access

Background

The Internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. As with any school resource, computing needs to be organised and managed to maximise its effectiveness and the contribution it can make to developing and supporting the educational policies of the school. Some of the information to be found on the Internet may be inappropriate for pupils, and it is wise to have a policy in place that takes this into account. This policy will help to define appropriate and acceptable use by both staff and pupils and offer a focus for continual debate.

1. The Internet in Abbey Court School

1. The use of the Internet enhances pupils' educational opportunities by offering unlimited access to information at the control of a switch. It offers pupils with learning difficulties wider opportunities to handle information.
2. The effective use of the wealth of material on the Internet will be monitored by the computing subject leader through access to the computer files; responses to questionnaires; monitoring planning and through staff meetings on a regular basis.
3. Internet use provides the opportunity to access up-to-date educational articles and information to the professional work of school staff. The school is enabled to stay at the forefront of curriculum development whilst offering its own expertise to a wider audience.
4. Abbey Court will endeavour to raise its profile through its communication with parents and through advertising of local community events to the local community.

2. The Internet in the Curriculum

5. Internet access is planned into the curriculum through the Schemes of Work. Additionally, the computing coverage plan will map out entitlement for access to computing by all pupils and ensure that individual capability is targeted and recorded effectively.
6. Abbey Court is aware that the pupils will be likely to access the Internet in a wide range of contexts both within, and outside school. Apart from using the Internet to support learning in the traditional school classroom, pupils will benefit from opportunities to access the Internet in lunchtime clubs, in youth clubs, public libraries and other community services, in Internet cafés and shops, and at home. Internet Access during the school day will be supervised.
7. The computing subject leader, reporting to the Senior Leadership and Governors will be responsible for developing pupil and staff research skills including the effective, reasonable and legal use of information retrieved.
8. Pupil's work will only be published on a website with prior agreement from the Senior Management Team. Termly the school newsletter is uploaded to the school website.
9. Pupils will be provided with an Office 365 user account which includes access to Outlook emails which is password protected. The use of E-mail by pupils in school will only be under the direct supervision of a member of staff, as will all other use of the Internet in school.
10. Pupils will be taught to follow sensible rules for personal safety. This is included in Abbey Court's Personal, Social and Health Education policy as well as the Computing policy. It is the responsibility of all staff to take responsibility for the development of basic skills as opportunities arise.

3. Responsibility

11. Pupils or staff should report receipt/access of unsuitable material to teachers. This should be treated as a child protection issue and reported as per the Abbey Court Child Protection policy and process. The Designated Safeguarding Lead (DSL) will review and report any pertinent information to the computing subject leader and/or Network Manager/IT Technician for action.
12. This policy will be distributed to parents in hard copy and is available on the school website at https://www.abbeycourt.medway.sch.uk/assets/Documents/Policies/Computing-Policy.pdf
13. Permission will be sought from parents before pupils are allowed Internet access using the parents' permission letter at the end of this policy which is included in the school's admissions documentation.
14. Staff and pupils are also required to sign the acceptable use statements at the end of this policy.
15. Training will be given to staff from the Designated Safeguarding Leads/Network Manager via INSET/briefings and on an ongoing basis as needed.

4. Internet Access

16. Access to the Internet is currently available in the school through a managed broadband service. This service monitors the appropriate use of the technology.
17. All pupils will be supervised by staff whilst accessing the Internet. For higher achievers who can access the Internet independently, individual arrangements and agreements will be made with reference to the computing subject leader.
18. The school's access to the internet is via Medway's Broadband systems which are managed as a contracted service by Atomwide. Atomwide provides a filtering system appropriate to the needs of schools.
19. The Network Manager is responsible for password security on all computers.
20. The Network Manager/IT Technician, reporting to the Designated Safeguarding Lead and Governors, will be responsible for compliance to DfE Keeping Children Safe in Education advice and guidance for Filtering and Monitoring September 2023 and Monitoring standards for schools and colleges, March 2023. They will ensure appropriate blocks are in place and regularly monitor internet usage on all school-owned devices.

5. The Legal Context

There is no legal definition of the term 'pornography' and there are few legal precedents relating to the use of the Internet. There are several laws which are likely to apply to the use of the Internet in certain circumstances including the Obscenity Acts of 1959 and 1964, The Protection of Children Act of 1978, The Indecent Displays Act of 1981, The Criminal Justice Act of 1988, The New Internet Defence Defamation Act 1996, The Data Protection Act 1998 and The Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000. The use of a computer system without permission or for a purpose not agreed by Abbey Court School could constitute a criminal offence under the Computer Misuse Act 1990. In many cases, laws relating to copyright, libel, obscenity or incitement to racial hatred are likely to apply to the use of the Internet.

In conclusion, while the legal position is not always well defined, there is a legal framework that could be applied to Internet use and new Acts continue to tighten up on Internet use.
Abbey Court School will ensure compliance with the guidance from DfE and Keeping Children Safe in Education (KCSIE) September 2023, London Grid for Learning (LGfL) policy checker and National College for Online Safety.

6. The Ethical Context

Abbey Court School recognises its overall moral responsibility and its duty to protect the pupils in its care. Parents expect Abbey Court to promote high standards in relation to the use of computers and the Internet whether or not the material being accessed is necessarily illegal.

The possibility of inappropriate use of the Internet by pupils or staff is something that needs to be well understood by Teachers and other staff, all of whom may come into contact with social media, the Internet or broadband apps through a range of different devices. Teachers may be faced with accidental access to inappropriate material during a lesson, or may encounter pupils who are explicitly/accidentally searching for such material. It is part of the school's responsibility to its staff to ensure that they are never placed in a situation for which they are not prepared and where they are unaware of the school's policies.

Section 3 - Strategies for preventing misuse of Internet access

a. Educational Strategies

As previously mentioned, there are two main approaches to Internet access, education and management. Pupils may be educated to develop a responsible attitude to computer and Internet use within and outside the school environment with the intention that pupils can make the right decisions if they understand the issues. Abbey Court School will also need to regulate Internet access. Pupils cannot be relied upon to foresee danger. Faced with suspect material, the pupils will not have the experience or maturity to make informed judgements. Internet access at Abbey Court is likely to be directly controlled by an adult working with a small group of pupils. For our higher achievers, a rules approach may be appropriate, whereby a code of conduct is agreed or set. Both types of approach, education and regulation, may be appropriate depending on the age and maturity of the pupils.

Pupils' use of the Internet may be greater at home than in school, and we may need to extend the educational approach to include parents where appropriate. Families may need to be helped to develop strategies to cope with the knowledge and influences introduced by the Internet and to understand the consequences for their child's life.

The Internet makes available an even wider range of material than CD-ROM, TV and video although many pupils still simply copy entire articles and images uncritically. Pupils' information handling skills in selection and in checking origin, currency and accuracy have become vital. Maturity in the application of this information will result from improved knowledge and awareness of the Internet.

b. Management Strategies

Within the curriculum planning process, management will review the contribution made by Internet use to teaching and learning. We wish to ensure that we have done everything reasonably possible to ensure appropriate and safe use of the Internet. (Which includes this internet access/e-safety policy).

IT systems are expensive and are becoming critical to efficient curriculum delivery as well as to school administration. To reduce any misuse of computer facilities, the school is allocating resources for the implementation of technical strategies and ensuring that they are effective.
By setting the criteria for use and access, staff and pupils will be reminded that the school's IT system has been installed to enhance and extend pupils' education.

The school will need to take a view on the degree of pupil autonomy in Internet access and the balance between privacy and control. The approach to supervision of Internet access will vary according to age and ability. (If a high achiever is allowed to access the internet alone then secure (see c. below) or agreed access will need to be considered).

Wherever pupils interact with the public by telephone, e-mail or website, particular care is required to ensure the communication is appropriate. Pupils need to follow sensible rules for personal safety, for instance never giving their full name, home address or telephone number. Appropriate use may take time to develop.

c. Technical Strategies

Technical solutions to social issues cannot be expected to be fully effective by themselves, but they should form an important part of a holistic approach.

Restricting access to inappropriate/unsuitable material is often the first issue to be tackled. Four overlapping approaches have evolved. These can be referred to as blocking, approved lists, filtering and rating, although these categories are often confused.

1. A blocking strategy generally removes access to a list of unsuitable sites or newsgroups. Maintenance of the list is a major task as it may contain thousands of sites, and changes must be made frequently.
2. An alternative strategy is to permit access only to approved sites - the *walled garden* approach, but it is difficult to predict the breadth of pupils' questions or search words, including the use of a different language.
3. Filtering examines the content of Web pages or e-mail messages for unsuitable words. The advantage is that no prior work is required, but there are problems, for instance with a Web page containing images only. Filtering of Web searches reduces pupils' opportunities to locate (inadvertently or otherwise) unsuitable material.
4. Rating systems give each Web page a rating for sexual content, profanity, violence and other unacceptable language or content. Web browsers can be set to reject any pages not rated appropriately for the pupil. At present few pages have been rated and, without a consistent international approach, rating is unlikely to become a viable strategy.

As new sites appear every day, none of these systems can be completely foolproof and a combination of approaches will be required. Our review will be ongoing of what is appropriate and whether the criteria used, suit the pupils in Abbey Court School and we have the following systems in place:

- Webscreen in line with LGfL (London Grid for Learning) which are a National/Regional support provider.
- We link to the National College of Online Safety.
- Staff are alert and regularly monitoring online usage; our filtering system blocks inappropriate content around Discrimination, Drugs/Substance abuse, Extremism, Gambling, Malware and Hacking, Pornography, Piracy and Copywrite, Self-harm and Violence in line with guidance from LGfL.
- Regular monitoring and daily awareness mean that we can block websites, trigger words, acronyms and Apps. The DSL and IT Technicians respond immediately to any reported/recorded concern via CPOMS.
- The IT Technicians run random filter test reports about website usage and review good sites as well as those which may cause concern. This is reported to the DSL.

- All staff have received training and are aware of how to record concerns using CPOMS. This is alerted immediately to the IT Technicians and DSL
- We use Cantium, which is owned by Kent County Council, and Atomwide, which is part of London Grid for Learning (LGfL).

Section 4 'Sexting': Definition and Advice

There are several definitions but for the purposes of this advice sexting is defined as:

Images or Videos that are sexual or are indecent and are generated

- by pupils, or
- of pupils

These images are shared by young people and/or adults via a mobile phone, handheld device or website.

Steps to take in the case of an incident:

1. Follow the standard child protection and safeguarding policies.
2. Record the incident and immediately report it to the Designated Safeguarding Lead (DSL)
3. Do not search a device, copy or print out 'evidence' simply inform the DSL who will decide upon the appropriate course of action.

Section 5 - Sensible use of emails/internet/mobile phones when driving: Applies to Private and School Phones

This guidance applies to all email/Internet use, whether it is at school, or at home.

Computer Viruses/hacking/scam emails/texts are a constant threat, and they are always evolving to "beat the system". Computer Viruses/hacking/scam emails/texts spread in a variety of ways, but with more and more people using the Internet and emails to communicate, this is the most common medium for the distribution of viruses or to target individuals with scam emails/texts. New viruses/scam emails and texts are found every day, so all of us need to be careful when opening/reading emails, and when using the Internet in general.

Common file extensions for viruses are .doc .exe .zip .pif .scr and .com (although there are others). The email/text message itself will normally consist of a short message along the lines of "Please see the attached file" or "Hey there, how are you doing" (although this message will vary). If this file is opened, it will 'infect' the machine, or device and the virus will do what it has been programmed to do, which is normally to restart your machine, delete files on your machine, and send copies of itself to as many other machines or devices as possible.

On a computer or mobile phone, to enable the virus to spread, it will look at your email/phone program's address book, and send an infected message to everyone you know (which is how you will often receive infected emails from someone you have regular contact with).

As a rule of thumb, it is best to delete any message that you are not sure of, especially if it has an attachment. You can often receive infected messages from people that you know, but you should be able to tell if the message is genuine or not.

When a colleague sends an email with an attachment, they will normally put your name at the start, a message in the middle, and their name at the end of the message. They would not normally just say "Look at the attachment".

If you are not sure about it, you should ask the person before you open it. If they say no – delete it!

Medway LA has virus detection software on the email system that detects *most* viruses before they even reach our inboxes, but unfortunately, it cannot block everything. Abbey Court also uses anti-virus software at IP level.

If you use your own email account at home, your email provider may have a similar system in place, but this is not always the case. Microsoft can provide useful information at windowsupdate.microsoft.com. It is also important that each machine that connects to the Internet has an up-to-date virus scanner installed. The virus scanner will alert you to any suspicious files and will help you get rid of any viruses that your computer may pick up.

Examples of commonly used anti-virus software are Norton Anti-virus, Sophos Anti-virus and McAfee Virus Scan (there are many others available from a variety of retailers).

Similarly, the same can apply to mobile phones so contact your network provider who can advise.

Summary:

- If you get any suspicious looking emails/texts – Delete them straight away.
- It should not harm your computer/mobile device if you just read an infected message. The harm is done when you open the attachment.
  Do not open any attachments you are not sure of.
- If you get a message from someone you know – try to compare it to the "usual" messages you receive from that person. If it just tells you to look at an attached document – it is probably a virus.
- Make sure you have an up-to-date virus scanner on your home machine.
- You should visit the Microsoft downloads site to ensure your home machine is always protected against known vulnerabilities in Windows and related software.
- Ensure you regularly update your phone software via your mobile phone provider. If you are unsure, contact your mobile phone provider for advice.

Introduction

Mobile phones are now seen as an essential means of communication. However, it is widely recognised that using a mobile phone whilst driving is unsafe, can distract the driver and could lead to an accident. Research has shown that drivers using mobile phones drove too close to the vehicle in front, failed to maintain speed control and wandered about on the road. All the available evidence shows that it is the conversation and not the physical act of using the phone that is the main distraction.

What does the Law say?

As of 1st December 2003, it is illegal for a person driving a motor vehicle on a road to use a hand-held mobile phone or hand-held device (except a two-way radio) that performs an interactive communication function by transmitting or receiving data. This is under the Road Vehicles (Construction and Use) (Amendment) (No.4) Regulations 2003.

It is also an offence under these regulations for an employer to cause or permit an employee to use a hand-held mobile phone or hand-held device.

Employees are reminded that it is an offence under the Road Vehicles (Construction and Use) Regulations 1986 for a person to drive a motor vehicle if they do not have proper control of the vehicle. This means you still risk prosecution of you use a hands-free phone or similar device when driving.

We are committed to providing employees with a safe place of work, including safe practices and procedures, and this includes the period employees are driving during the course of their work.

Employees must not use a hand-held mobile phone while they are:

- Driving;
- Stopped at traffic lights;
- In a traffic jam or any other form of traffic hold-up; and,
- In any other unsafe location.

Use of a hand-held mobile phone includes using any function on the phone such as text messaging and the use of any mapping apps.

A mobile phone consisting of a wire and an earpiece is not classed as hands-free and must not therefore be used whilst driving.

Employees should ensure before they commence their journey that either the phone is switched off or the messaging service/voicemail/call divert is switched on. If an employee inadvertently forgets to comply with this and the phone rings whilst they are driving they should not answer the phone and return the call when safely parked (i.e. With the engine switched off).

Employees are encouraged to take frequent breaks from driving for extended periods and to check for messages during those breaks.

The only time an employee is permitted to use a hand-held mobile phone whilst driving is to call the emergency services on 112 or 999 in response to a genuine emergency and where it would be unsafe or impracticable to stop driving to make that call. Where possible, another adult passenger should be, making use of the school mobile phone which is taken out on any off-site educational visit.

All the above also applies to the use of a hand-held device (except a two-way radio) that performs an interactive communication function by transmitting and receiving data.

The use of a hands-free mobile phone (installed in a recognised hands-free kit) and two-way radios whilst driving is not prohibited under this policy. However, as research has indicated that it is the conversation that is the main distraction, hands-free kits should not be supplied to employees unless there is a genuine and real operational need for the employee to be contactable by phone whilst driving. If this is the case a risk assessment must be made by the manager to identify the most appropriate kit to be fitted and the employee trained in its use. All employees who use these devices must still comply with the principles of safety that underpins this policy and wherever possible find a safe place to stop when they are in use.

If an employee rings someone and it becomes apparent the person is driving the employee must politely check if they are using a hands-free mobile phone and if not, terminate the call immediately, suggesting the person parks safely and rings them back.

Monitoring and Review

This corporate policy must be communicated at both a corporate and directorate level to ensure all employees are aware of its contents. This policy will be reviewed after the first year of implementation to assess the effectiveness of the measures introduced and then on a 3-yearly basis or after a significant event whichever is the sooner.

At Abbey Court School blue tooth is available for the use of the Senior Leadership Team. No other staff are asked or required to use a mobile phone whilst driving.

Mobile phone cameras

For the purpose of safeguarding children and confidentiality, staff must not use their mobile phones whilst in school (including educational visits; work experience; inclusion etc.). The school provides digital cameras for this purpose. The use of a personal Mobile Phone to take photos of pupils in any context would also be a breach of confidentiality and would lead to disciplinary action.

Mobile phones can only be used in agreed areas i.e. the staff room and areas of the premises outside of the main building.

The use of 'map' apps

If it is deemed necessary to use, and follow a digital map when on an educational visit, then this must be done in a careful and considered way. The device must be set up before the trip has begun and whilst the mode of transport is stationary. The mobile phone must be mounted using a secure, hands-free device. The driver should not interact with this device whilst the mode of transport is moving. The app must use a voice output method, with the directions being spoken aloud.

Related Policies
Confidentiality Policy
Complaints Procedure
Safeguarding and Child Protection Policy
Equality, Diversity and Inclusion Policy
Computing Policy (Curriculum Handbook)
Disciplinary procedures (School Handbook)
Data Protection (School Handbook)

APPENDICES

Abbey Court School

Acceptable Internet Use Agreement for Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Acceptable Use Agreement has been drawn up to protect users.

The school reserves the right to examine or delete any files that may be held on its computer network system or to monitor any Internet sites visited including on any portable devices owned and provided by the school for staff to use for school purposes. The Network Manager/IT Technician recall devices at least twice a year for updates and checks;

You are agreeing to the following:

- All Internet activity via the school network, should be appropriate to staff's professional activity or the student's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person at any time;
- When accessing/completing work from home, you must maintain confidentiality at all times and lock your computer when you are away from it;
- Whilst it is not practical nor appropriate to restrict access to the internet by the staff at home, any school information remains confidential and must not be shared or published via the internet. This will constitute a breach of confidentiality (reference the Confidentiality Policy).
- Activity that threatens the integrity of the school computing systems, or activity that attacks or corrupts its, or other systems, is forbidden;
- The use of school computing systems for sending private e-mails is prohibited at all times and the school has the right to monitor the school systems to ensure adherence to this agreement.
- Users are responsible for ensuring compliance to this agreement for all e-mail sent and
- Where a school device is used to access personal emails, you are responsible for insuring nothing inappropriate is downloaded to the device.
- Where a personal device is used to access work emails, you are responsible for abiding by the same rules which apply to the use of a school device as outlined in this Agreement.
- As e-mails can be forwarded, intercepted or inadvertently be sent to the wrong person, the same professional use of language and content should be applied as for letters or other media used in school;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the school network or a school device, to intentionally access inappropriate/unsuitable materials such as pornographic, racist, drugs or offensive material is forbidden.
- Where inadvertent access to inappropriate/unsuitable website(s) occurs, staff must report this immediately to the Network Manager/IT Technician.
- Staff must be aware that involvement in discussion groups, blogs and social network systems (e.g. Facebook and Instagram) should be for personal interest only and not offer opinion, view or photos that could bring the reputation of the school into disrepute. The discussion of issues and information pertaining to Abbey Court School, would be a

breach of confidentiality and would lead to disciplinary action. Linking on social media with a parent(s)

of the school is discouraged unless these are family members. Any such link should be notified to the

Headteacher.

Full name:_____

Signed:_____ Date:_____

Parents' permission letter

Dear Parent/carer,

Internet Permission Form

As part of the school's 'Computing' programme we offer pupils supervised access to the Internet. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the form below, as evidence of your agreement and their acceptance of the school's rules on this matter.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using social media and information sources. To that end, the school supports and respects each family's right to decide whether or not to give permission.

Our school has a secure and robust filtering system, and we have monitoring processes in place. Our staff are trained to notice any websites/programmes that are not appropriate/suitable for the pupils to be accessing. There may be times when new websites may appear that our filtering system is not yet familiar with. The pupils are specifically taught about Internet/Online/E-Safety, and are always supervised by an adult when accessing the Internet.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We would be grateful if you could read the attached Policy, which can also be found on our website, and then complete and return the permission form below.

Yours sincerely

Vicky Aspin
Headteacher

Internet Parent Permission Form

Please complete and return this form to the Headteacher.

Pupil Name: _____

As a school user of the Internet, I agree to follow the school rules on its use. I will use the School's ICT system and Internet in a responsible way and observe all the restrictions explained to me by the school.

Pupil Signature _____ Date: _____/_____/_____
(Sign by, or on behalf of, the pupil)

Parent/Carer

As the parent or legal guardian of the pupil signing above, I agree that my child can use the school's ICT system and internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for child to follow when selecting, sharing and exploring information and media.

Parent/Carer Signature: _____ Date ___/_____/_____

Parent/Carer Name: _____