Fellgate Primary School

Together Everyone Achieves More

Online Safety Policy

Document Control

Document Name	Online Safety Policy
Version	4.0
Linked Documents	Data Protection Anti-Bullying Child Protection and Safeguarding Policy Healthy Schools Behaviour Policy Acceptable Use Policy
Date Published	February 2018
Review Date	January 2025
Audience	Staff, Parents and Governors
Approved By	Governing Board

Change History

Version	Date	Issuer / Amender	Changes Made	Approval
1.0	February 2018	S. Mcmullen	Policy brought in line with policy standards	Governors
2.0	October 2020	A.Hearn (Computing Lead)	- Vision statement added. - Updates linked to KCSIE 2020 and the DfE 'Safeguarding and remote education during coronavirus (COVID-19)' guidance. - In response to the potential requirement for schools and settings to continue to offer remote learning following full or partial school closures, this document has been updated with remote learning guidelines for staff and learners and updated AUP for staff, pupils and parents.	Governors
3.0	November 2022	A.Hearn (Computing Lead)	Pg 14- Portable Storage Devices: The use of USB sticks are strictly prohibited in school. Pg 14: Staff mobile phones Pg 23- Updates from KCSIE 2022 document	Governors

4.0	January 2024	A.Hearn (Computing Lead)	- Policy named changed from 'E-safety' to 'Online Safety' Policy. - Separated the Acceptable Use Policy. - Updates linked to KCSIE 2023. - Filtering and Monitoring updates added. - Staff training section added.	Governing Board/HT

Contents

Our Vision

At Fellgate Primary School through an ethos of respect, challenge and resilience, we aspire to create an inclusive, safe, vibrant, happy school where each member of the school community - children, parents, carers, staff and governors - feels valued and are encouraged to be the best they can be.

We celebrate individuality, striving for everyone to reach their full potential and "shine" in everything they do.

Our Values

We **respec**t ourselves and others, encouraging everyone to be the best they can be.

We thrive on **challenge** so that we can all reach our full potential.

Resilience- We never give up and understand that it is ok to make a mistake.

Inclusion- Every member of our school community has a voice, are listened to, appreciated and supported.

Unique – we all have different strengths and abilities and are special in our own way.

Our Aims

To create caring, confident and curious children who are successful learners, confident individuals and responsible citizens.

To motivate and challenge our children to achieve academic and personal success.

To appreciate the uniqueness of each child and recognise their potential.

Chair of Governors: Mrs J Price	Head Teacher: Mrs J Tones
(Print Name)	(Print Name)
Signed: *J Price*	Signed: *J Tones*

Context

Development of this Policy

Our online safety policy has been written by the school, building on the guidance provided by ICT in Schools and Smoothwall. It will be reviewed annually. The online safety policy is part of the school development plan and relates to other policies as stated above.

Aims

This policy aims to ensure that all pupils, including those with special educational needs:

- Will use the internet and other digital technologies to support, extend and enhance
- their learning.
- Will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material.
- Will develop a positive attitude to the internet and develop their computing capability through both independent and collaborative learning.
- Will use existing as well as new technologies safely.
- Will know who to speak to when they feel unsafe when using communications technology.
- Will know how to report any abusive behaviour they experience online.

This policy is intended to help provide clarification on unacceptable behaviours, relating to any information and communications technology owned by the school, or personal technology used within the context of the school (this includes off site visits, using school systems at home etc.).

It aims to cover all computing including: -

- the use of computers on the school network, filtering and monitoring
- all mobile devices including laptops, ipads, mobile phones, desktop computers and audio/visual equipment
- electronic communication and storage systems
- raising awareness of online safety among pupils, staff and parents
- offering guidelines which will safeguard and protect pupils and staff from misuse of technology
- This policy applies to all teaching staff, support staff, pupils, governors, visitors and volunteers.

Teaching and Learning - Benefits of Technology

The internet and other digital technologies are an essential element for education, business and social interaction. The school has a duty to embrace such technologies and provide pupils with quality access and guidance, as part of their learning experience. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning so the school access will be designed expressly for pupil use and includes a robust filtering and monitoring system.

Internal networks and electronic communications, audio visual equipment, laptops, iPads and PCs are an essential part of the educational environment. The whole school community needs to understand the appropriate and effective use of such technologies, to support teaching and learning.

Risks Associated with Using Technology

There are unfortunately risks associated with the positive educational and social benefits of using the internet and other digital technologies.

Pupils will therefore be:

- taught what internet use is acceptable
- be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- taught what is not acceptable and be given clear objectives and guidelines for the use of the internet and other digital technologies
- taught how to keep themselves safe online

Fellgate Base

The principles of this policy will be embedded into the philosophy of the Base, however, due to the specialised needs of the children, the strategies and actions need to be differentiated. These should be based on the knowledge of the child and the expertise of the adults.

Managing the School Network and Internet Access

System security, filtering and monitoring

Managing the system

- The school's computing systems security will be reviewed regularly by Smoothwall. Weekly updates are sent to the DSL and deputy DSL's.
- Filtering and monitoring procedures will be reviewed at least annually.
- The online safety coordinator is responsible for ensuring that the policy is implemented, updated and complied with. The online safety team will support this.
- The online safety coordinator will ensure that the school community is kept up to date with safety issues and guidance in collaboration with Smoothwall, ICT in Schools and child protection authorities.
- The school will work in partnership with Smoothwall and ICT in Schools to ensure that filtering and monitoring systems are effective as possible.
- The technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- If staff or pupils come across unsuitable online materials, the site must be reported to the online safety coordinator.
- The online safety coordinator will ensure adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures are applied that provide for continuity of ICT security when staff vacate or occupy a post:
    - a record that new staff have been issued with. have read the appropriate documentation and have signed the acceptable use policy. These are held with the secretary.
    - a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment. School network access will be closed immediately on the termination of employment by a member of the online safety team.

  The school maintains the right to regularly monitor internet traffic, the school's network and user email. We are obliged to monitor to fulfil our responsibilities with regards to UK law.

Passwords

All users must observe password protocols for network and internet access.
Passwords for staff users should be changed at least termly and should not be reused. They should be a minimum of 6 alphanumeric characters and not obviously guessable.
Users must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the system manager to issue a new password.
A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur.
A password to access the internal network must not be shared.

Private Hardware and Software

Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes is approved by the System Manager.

Equipment Siting

Reasonable care is taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users observe the following precautions: -

Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be

given to the siting of devices on which confidential or sensitive information is processed or retrieved.

Equipment is sited to avoid environmental damage from causes such as dust & heat.

Users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users. Users should not allow other staff or children to access their account.

Users have been instructed not to leave hard copies of sensitive data unattended on desks.

The same rules apply to school equipment in use at a user's home.

Virus Protection

The school uses appropriate anti-virus software for all school computing systems.

The school ensures that every user is aware that any computer with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.

Any third-party laptops not normally connected to the school network must be checked by the System manager for virus' and anti-virus software before being allowed to connect to the network.

Teachers must take the necessary steps to ensure anti-virus protection software on their laptop is updated on a weekly basis as a minimum.

Disposal of Equipment

Disposal of waste computing media is made with due regard to sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it can be derived.

Prior to the transfer or disposal of any computing equipment the system manager ensures that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any computing equipment must be disposed of in accordance with WEEE regulations.

Repair of Equipment

If a machine, or its permanent storage (hard drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on a portable drive for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data

Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

Staff Training

- DSL's will receive termly smoothwall training to keep abreast of changes and updates.
- All staff will receive annual online safety training.
- All staff will understand the difference between filtering and monitoring.(Filtering systems block access to harmful sites and content. Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school devices. School is then alerted to any concerning content so school can intervene and respond)
- The computing lead/online safety coordinator will attend termly network meetings and attend all training sessions pertaining to online safety. This information will be disseminated back to staff.

Communication

School Website, Email, Google Classroom and Class Dojo

Pupils and staff may only use approved e-mail accounts in school. You must use the e-mail address issued by the school for employment purposes only. Pupils have access to email and messaging through the school network and Purple Mash programme.
Staff must only communicate with pupils, parents/carers using official school systems. Any such communication will be professional in tone and manner.

Managing Approved Email Accounts

All users who log on to the school website and school email system at home or at any other location, must only use these systems for educational use and are bound by the acceptable use guidelines.
The school has the right to monitor e-mails and internet use.
No users should ever use the school's communication systems to access or send inappropriate materials such as pornographic, racist or offensive material or to send or forward anonymous messages and chain letters.
Users should not access public chat rooms and messaging systems unless permission is given from the online safety coordinator. Staff are permitted to use YouTube within school for educational purposes.
Pupils and staff must treat emails with links or attachments as suspicious and not open any links unless they know they are safe.

Users should not use the school's communication technologies for personal financial gain, gambling, political purposes or advertising.
Users will be advised to never disclose personal details such as name, address, age or telephone number.
Whole class or group email addresses should be used at Key Stage 1 or below.
Any inappropriate communications received must be reported to a member of staff immediately.

Accessing Internet Sites

Users should not visit sites that contain illegal, obscene, hateful or other objectionable material.
Users should use the school's internet for professional/educational purposes only and not for personal reasons within school time.
At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
At Key Stage 2, pupils should not be allowed to 'surf' the internet freely. They should be given specific sites to access or clearly defined and closely directed activities.
Teaching staff should always research potential sites before directing pupil activities.
Staff will always use a child friendly safe search engine when accessing the web with pupils

School Website, Media Publications and Videos

The following protocols will be observed: -

Staff and pupil contact information will not be published. The contact information given, will be that of the school office.
The online safety lead will take overall editorial responsibility to ensure that content is accurate and appropriate.
Authorisation needs to be gained from the e-safety coordinator in order to publish information on the internet.
Any images that involve children must not identify the children by name. Group photographs may be used where appropriate.
The permission of parents will be sought, before photographs or work is published on the school website, school social media, in media publications, on class dojo, or in school videos. (A record of each child's permission slips for each class are kept in the school office)

Managing Video Conferencing & Webcam Use

Video conferencing should use the educational broadband network to ensure quality of service and security.
Pupils must ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing and webcam use will be appropriately supervised for the pupil's age. Webcams should be checked and monitored to ensure that misuse does not occur accidentally or otherwise.

Remote Learning Guidelines

These remote learning guidelines have been put in place to safeguard all members of Fellgate Primary School when taking part in remote learning following any full or partial school/setting closures.

Remote learning will take place using Google Classroom and Class Dojo. Video calls will only be made using Google Meet. These systems have been approved by the e-safety coordinator.
Staff will only use school managed or specific, approved professional accounts with learners and/or parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
Staff will use work provided equipment where possible e.g. a school laptop or ipad.
Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by the head teacher: 9am-3pm.
All remote lessons will be formally timetabled (using google calendar) so the head teacher or a member of SLT is able to drop in at any time.
Any personal data used by staff and captured when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by the head teacher and in line with our data protection policy requirements.
Appropriate privacy and safety settings will be used to manage access and interactions.
A pre-agreed invitation/email through google meet detailing the session expectations will be sent to those invited to attend:

- Access links should not be made public or shared by participants. If relevant to the system being used.
- Pupils and/or parents/carers should not forward or share access links.
- Pupils are encouraged to attend lessons in a shared space or in a room with an open door so they can be appropriately supervised by a parent/carer or another appropriate adult.

All participants are expected to behave in line with existing school policies and expectations.
Staff will remind pupils of behaviour expectations and reporting mechanisms at the start of the session.
If inappropriate language or behaviour takes place, pupils involved will be removed by staff, the session may be terminated, and concerns will be reported to the head teacher via CPOMS.
Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

Any safeguarding concerns will be reported to the head teacher via CPOMS in line with our child protection policy.

Social Networking, Instant Messaging and Personal Publishing

The term 'social networking' refers to online communities where typically text, photos, music, video are shared by users. Instant messaging refers to online chatting to others in 'real time'.

Class Dojo connects teachers, students and families through communication features, such as a feed for photos, videos and messages. This method of communication is approved by the e-safety coordinator and governors.

The school will not normally allow staff and pupils access to any social networking and instant messaging sites that are not approved of by the e-safety coordinator.

Staff, pupils, parents and carers must not put photographs of other people within a school context on social networking sites without their permission. Parents are advised when taking photographs of plays, performances, etc. that they are not to publish them on social networks.

All staff should be aware of posts, photographs and 'friend requests' and how they may reflect on the reputation of the school.

The online safety team will monitor the school's Facebook account.

The school is aware that there are risks associated with using social media such as, reputation damage, data leakage etc. so a 'Social Media Risk Assessment' (Appendix) will be completed annually to assess the effectiveness of the control measures in place.

Newsgroups will be blocked unless a specific use is approved.

The school does accept that there can be educational benefits (e.g. collaborative work nationally and internationally) and will therefore examine their use for teaching and learning as the need arises.

The school will consider how to educate pupils in their safe use.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames, gamer tags and avatars when using social networking sites and playing games.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Data sensitive files will be stored in a central 'lockable' space in both buildings. Correct storage of pupil information follows the guidance in the data protection act and Fellgate Primary's Data Protection Policy.

No personal data files are to be transferred onto USB sticks.

Copyright and Plagiarism

The school will ensure that copyright and intellectual property right laws are not infringed. Pupils will be taught to reference all material used from the internet and other sources, as they develop their research skills.

Mobile Phones

Taking Digital Images Using Cameras and Videos

It is recognised that the taking of digital images is an integral part of the teaching and learning experience, but there must be a clear educational reason for creating, storing, distributing and/or manipulating images of members of the school community.

Staff and pupils may take digital photographs or videos using school equipment, providing that they support educational activities. Images from school devices must be removed and placed on the school network as soon as practically possible.
Images/video should not be taken with personal mobile phones or cameras (e.g. whilst on school visits). However, in exceptional circumstances this may be permitted with the approval of the e-safety team. Any images must be transferred to the school network within 24 hours.
All images of children stored on the school network or on staff laptops should be placed in a common folder with a clear explanation of the intended use of the images, not in the personal areas of staff or other users of the systems.
Pupils' names should not be used when saving images.
Images should be deleted from laptops and PCs at the end of the academic year, unless retention is approved by the online safety co-ordinator.
Pupils will be taught how images can be misused, through their e-safety learning.

Mobile Phones

Pupils should not bring mobile phones into school. In exceptional circumstances, a written request may be sent to the head teacher. If approved, the phone will be stored in a central place until home time.
Pupils will be advised that the sending of abusive or inappropriate text messages or files is forbidden.
Staff will keep personal phones secure and these are not to be used in lessons or in front of children. They are not to be used in teaching sessions, but can be used in the staffroom at break times.

Laptops

Staff should store school laptops in a secure location overnight.

If school laptops/ipads are taken home, staff are responsible for their security.
School laptops/ipads are for sole use of the staff member to which they are loaned and not to be used by other members of the household.
The school IT technician is responsible for maintenance of school laptops/ipads and no other person should tamper with them.

Portable Storage Devices

The use of USB sticks at Fellgate Primary are strictly prohibited in school.
Pupils are also not allowed to use their own devices. These are blocked on children's accounts.

Games Machines

Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
Staff should check that gaming software is age appropriate if machines are allowed (e.g. fun/toy days).

Film/DVD

These should be age appropriate, as outlined by the film classification authority. Only films rated 'U' should be shown in school unless permission has been sought from the parents to watch PG films. The class teacher must take responsibility for this as and when this issue arises.

Assessing Risks and Handling Online Safety Issues

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.

The school will audit computing use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Reporting Procedures

Reporting Accidental Access to Inappropriate Material

Any user of the school who accidentally comes across inappropriate or offensive material should do the following: -

1. Inform the online safety coordinator/team member of the incident and give the website address.
2. Log the web address, time and username in the online safety incident log. This is kept in the 'resources file' on the school network.
3. The school should block the website via its own cache pilot or other proxy server.
4. The online safety coordinator should contact ICT in schools if the incident needs escalating. All children will also be taught how to report an issue.

Reporting Accidental Access to Illegal Material

Any user who accidentally comes across illegal material should do the following: -

1. Report the incident to the online safety coordinator or online safety lead.
2. Do not show anyone the content or make public the URL.
3. Make sure a reference is made of the incident in the e-safety incident log (saved on the network in resources)
4. Go to the IWF website at www.iwf.gov.uk and click the report button.
5. If reporting a URL don't use copy and paste, type the URL.

Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the network should take the following action: -

1. Report in confidence to the head teacher.
2. The head teacher should inform the Local Authority.
3. The Local Authority should complete an internal RIPA form, requiring the completion of an internal investigation.
4. If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, the local authority will inform the relevant police authority who will complete their own investigations.
5. If the investigation confirms that inappropriate behaviour has occurred, Northern Grid will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Examples of Inappropriate Use:

Visiting pornographic sites
Causing offence to religious groups
Inappropriate use of email

Deliberate sabotage of the network; i.e. hacking, mail bombing etc.

Access to Illegal Material

If this investigation results in confirmation of access to illegal materials or the committing of illegal acts Smoothwall will inform the relevant police authority that will complete their own investigations and a criminal investigation may follow.

Examples of Illegal Acts: -

Accessing any child abuse images.
Incitement to racial hatred
Incitement to violence
Software media counterfeiting or illegitimate distribution of copied software.

Sanctions

Sanctions for the abuse or misuse of school computing systems will be determined by the senior management team or the e-safety coordinator and governors of the school, as deemed appropriate.

Key Contacts:

Mike Hamilton (Local authority online safety contact for schools) Tel: 0191 4272123 email: mike.hamilton@ictinschools.org

Authorising Access

Authorising access to the internet and other computing resources.

All staff and pupils must read and sign an acceptable use policy before using any school computing resource. (found in school office)
Parents will be asked to sign and return a consent form relating internet access and the taking of digital images/videos.
The school will maintain a current record of all staff and pupils who are granted access to school computing systems.
Any person not directly employed by the school will be asked to sign an acceptable use of school computing resources before being allowed to access the internet from the school site. (found in school office)

Community use of the Internet

The school will liaise with local organisations to establish a common approach to online safety.

Communicating this Policy

Introducing the Online Safety Policy to Pupils

A programme of training in online safety (in its broader sense) is embedded within the computing scheme of work, the Personal Social and Health Education (PSHE) curriculum and is also covered by the Kidsafe UK program delivered by the schools Kidsafe tutor.
Online safety rules for school systems and equipment will be posted in all rooms where computers are used and discussed with pupils regularly.
Pupils will be informed that network and internet use will be monitored and appropriately followed up.
All children will sign an acceptable use policy, once in EYFS, KS1 and another when they move into KS2. The acceptable use policy are displayed in classrooms and the computing suite.

Staff and the Online Safety Policy

All staff will have access to the school online safety policy via 'Resources' and its importance explained. It is also displayed on the school website.
Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
Staff that manage filtering systems or monitor ICT will work with management and the LA to establish clear procedures for reporting issues.

Enlisting Parents' and Carers' Support

Parents and carers will be referred to the school online safety policy in newsletters, the school brochure, class dojo and on the school website.
The school will maintain a list of online safety resources for parents/carers and share these via the school website and class dojo. School will also promote online safety annually during online safety week and the globally celebrated 'Internet Safety Day'.
Parents are informed by letter about current safeguarding programmes developed in school, such as Kidsafe UK and they are kept up to date about what the children have been learning about.
The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school (found in the school office).
Parents and carers will be offered advice on online safety on an individual or group basis when needed. Parents are contacted if their child is involved in an online safety issue. Issues are recorded on cPoms.

Appendices

Legislation

Schools should be aware of the legislative framework under which this online safety policy guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

Erase or amend data or programs without authority;
Obtain unauthorised access to a computer;
"Eavesdrop" on a computer;
Make unauthorised use of computer time or facilities;
Maliciously corrupt or erase data or programs;
Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of an individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that person data must be:

Fairly and lawfully processed.
Processed for limited purposes.
Adequate, relevant and not excessive.
Accurate.
Not kept longer than necessary.
Processed in accordance with the data subject's rights.

Secure.
Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures. Communications Act 2003 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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Regulation of Investigatory Powers Act 2000 It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

Establish the facts;
Ascertain compliance with regulatory or self-regulatory practices or procedures;
Demonstrate standards, which are or ought to be achieved by persons using the system;
Investigate or detect unauthorised use of the communications system;
Prevent or detect crime or in the interests of national security;
Ensure the effective operation of the system.
Monitoring but not recording is also permissible in order to:
Ascertain whether the communication is business or personal;
Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered TradeMarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study.

The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Protection of Children Act 1978

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 pseudophotographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

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. (Typically, teachers, social workers and health professionals staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

The Education and Inspections Act 2006

Empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students/ pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Regulation of Investigatory Powers Act 2000

Also referred to as RIPA. This act is concerned with regulating the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. It was introduced to take account of technological change such as the growth of the Internet and strong encryption. In a school situation this would be requested if you or the LA or another law enforcement agency contacted you with suspicions that the school network was being used for illegal purposes eg: gaining access to potentially illegal material e.g. Child abuse images, or is suspected of inappropriate Internet / email use.

Keeping Children Safe in Education 2023

Also referred to as KCSIE. This is statutory guidance from the Department for Education (the department) issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

Pupil Consent Form – Fellgate Primary School

Please place a tick in your desired option:	Granted	Denied
Taking my child out of school for local visits within South Tyneside (this will include entering the child's details on the LA evolve risk assessment system)		
Taking my child out of school for local visits non-South Tyneside (this will include entering the child's details on the LA evolve risk assessment system)		
For my child to receive first aid or medical treatment either within the school or on school trips.		
For my contact details to be used for school text services		
Taking my child to visit places of worship		
Allow use of photographs/videos within the school premises		
Allow use of photographs/videos for use on the school website, on school's social media (facebook) and within school publications(such as newsletters).		
Allow the use of photographs/videos on class dojo		
Allow use of photographs for use in local press		
Allow use of photographs for use in national press		
Allow my child to use the internet under supervision on the school premises		
Allow my child to use the internet under supervision at another place of study		
Allow the school to provide the secondary school of your choice personal details about your child before the child begins at the school (year 6 children only)		

Permit the school to use my child's personal information for school leaving reasons such as leavers hoodies, etc (year 6 only)		

Child's Name: _____ **Class:** _____

Parent/carer Signature: _____ **Date:** _____

You can withdraw consent at any time by contacting the school and requesting a new consent form. If you would like any further information regarding the above, please contact the school.

Please return this form to school for our records.

Dear Parent/Carer,

We have had an increasing number of children bringing mobile phones into school. We appreciate that some parents may need to contact the children after school and so if your child must have a phone, we ask that you complete the form below.

As part of our online safety policy phones must be turned off on entering the school grounds and handed into the office.

Inappropriate use of mobiles may result in the device being kept in the office to be collected by a parent.

Yours sincerely

Mrs J Tones

Mobile Phones in School

I give permission for …… (child's name) to have his/her mobile phone in school.

I will turn my phone off when I come into school and hand it into the school office

Signed…… (Child's signature)

Signed …… (Parent/Carer signature)

Fellgate Primary School, Oxford Way, Fellgate Estate, Jarrow, Tyne & Wear. NE32 4XA
Tel. 0191 4894801 Primary School Tel. 0191 4837879 Autistic Base. Fax. 0191 4837109

Email: info@fellgate.s-tyneside.sch.uk

Social Media Risk Assessment for Schools

Hazard	Who it will affect	Control Measures to Reduce Risk	Any Further Action Necessary	Risk Rating Low/Med/High
Reputation	All	• A small number of named members of staff have responsibility for posting to the website and school social media sites. • Monitor any posts made about the school and be proactive in asking for removal if defamatory. • If staff can post to school website some sites are automatically linked to post to other social media sites. Staff should be mindful of this.		High at all levels.
Representation	All	• Monitor web for sites being created as school or members of staff. • Report any suspicious activity to the social media site concerned.	Consult legal team if libellous.	Low threat and likelihood, high vulnerability and impact.
Harassment	All	• Encourage disclosure of any harassment. • Meet with affected parties if possible. • Ask for apologies and removal of posts. • Revision of AUP's for all stakeholders. • Meet with the union representative if a staff member is involved. • Contact police if the situation is not resolved.	Online safety training and awareness for all stakeholders.	High threat and impact, medium vulnerability and likelihood.
Information leakage	All	• No personal, financial or sensitive material to be posted online on an unsecured site. • All students must have permissions for work and images to be posted online. • Refer to Data Protection policy.		Low, but high impact

Data loss	Selected members of staff	• Data should be hosted on a secure site not on social media. • Refer to Data Protection policy.		Low
Privacy	All	• No information relating to personal details to be posted online. • Ensure privacy settings on social media sites are set at the highest possible level. • Regularly check settings. • Where possible make the school social media site impersonal and not linked to a staff member's personal profile.		Low but high impact
Passwords	Selected members of staff	• Only selected members of staff to have logins to social media sites. • Make passwords robust. • Change passwords according to protocol in staff policy. • Passwords not to be shared or told to another user.		Low but high impact
Permanence of content	All	• On those sites that the school control such as their school website, older posts can be archived or removed. This does not mean they have disappeared from the web entirely as the pages may have been archived. • On sites such as Facebook and Twitter etc. content ownership is with the site.		Medium but low likelihood
Content and ownership	All	• Content ownership is with social media sites such as Facebook or Twitter and users agree on signing up to relinquish their control of content.		Medium threat and vulnerability, low likelihood and impact
Piracy and infringement	All	• All content posted should comply with legal regulations.		Low
Copyright	All	• All content posted should comply with copyright regulations.		Medium threat and vulnerability, low likelihood and impact

Virus and Malware	All	• Don't accept any files or friend requests. • Be wary of shortened URL's. • Don't download any multimedia content or applications from a social media site.	Ensure virus checking software is enabled, up to date and running.	Low
Purchasing from applications and games	All	• Don't download any games or applications from a social media site.		Low
Scam and phishing	All	• Don't complete online forms, surveys or supply log in details. • Don't share posts or competitions from commercial sites.		Low
Employment	Selected members of staff	• Don't advertise vacancies on unsecured social media sites.		Low
Overuse	All	• Refer to Acceptable Use Policy.		Low

Dealing with an online safety incident