Fellgate Primary School

Together Everyone Achieves More

E-Safety / Acceptable Use Policy

Document Control

Document Name	**E-Safety / Acceptable Use Policy**
Version	**2.0**
Linked Documents	**Data Protection, Anti-Bullying, Child Protection and Safeguarding, Healthy Schools**
Date Published	**October 2020**
Review Date	**October 2022**
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

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.

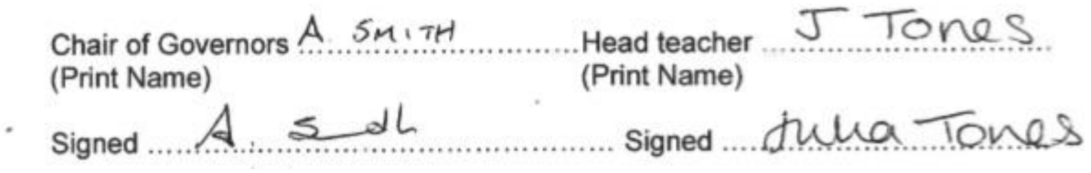
Unique – we all have different strengths and abilities and are special in our own way.

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 A. SMITH .... Head teacher J Jones ....
(Print Name) (Print Name)

Signed A. .... Signed Julia Jones

Context

Development of this Policy

Our e-Safety/Acceptable Use Policy has been written by the school, building on the guidance provided by the Open Zone, Durham County Council (Durham Net) and LA. It will be reviewed annually. The e-Safety/Acceptable Use Policy is part of the School Development Plan and relates to other policies, including Anti-bullying, Child Protection and Safeguarding, Data Protection and Healthy Schools.

Aims

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.
- network and internet connectivity.
- all mobile devices including laptops, iPads, mobile phones, desktop computers and audio/visual equipment.
- all software, electronic communication and storage systems.

It applies to: -

- staff (teaching and non-teaching)
- pupils
- governors
- parents helping or studying in school
- visitors

Teaching and Learning - Benefits of Information and Communications 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 expressively for pupil use and will include filtering appropriate to the age of pupils.

Internal networks and electronic communications, portable storage devices, audio visual equipment, laptops, iPads and PCs have become 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 Information and Communications Technology

There are unfortunately some 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 Autistic 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 unique to each child. 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

- School computing systems security will be reviewed regularly by eSafe.
- The e-Safety Co-ordinator is responsible for ensuring that the policy is implemented, updated and complied with. The e-safety team will support this.
- The e-Safety Co-ordinator will ensure that the school community is kept up to date with safety issues and guidance in collaboration with the LA, Open Zone and Child Protection authorities.
- The school will work in partnership with, the Open Zone, and Durham Net, to ensure that filtering systems are effective as possible.

- Fellgate Primary uses Durham County Council's Network and Service to access the broadband internet. We are required to comply with Durham County Council's Acceptable Use Policy (AUP) which must be signed and agreed by the Head Teacher.
- Senior staff 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 on-line materials, the site must be reported to the e-Safety Coordinator.
- The e-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 relating to ICT security, and have signed the list of rules. 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 e-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.
- Where a password to boot a PC or access to an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network.

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 ICT user is aware that any PC 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's 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 ICT media such as print-outs, data CD's etc. 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.

Communication

School Website, E-Mail, Google Classroom and Class Dojo

- An adult's personal Email account can be accessed in school providing they do not open attachments from unknown sources and not within class time or when children are in the classroom.
- You must use the e-mail address issued by the school for employment purposes only.
- Staff must only communicate with pupils, parents/carers using official school systems. Any such communication will be professional in tone and manner.
- Pupils are not allowed to access personal email accounts from the school network at any time. Pupils have access to email and messaging through the school network.

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 given from e-safety coordinator. Staff are permitted to use YouTube within school for educational purposes.

- 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 Web Site, Media Publications and Videos

The following protocols will be observed: -

- Staff and pupil contact information will not generally be published. The contact information given, will be that of the school office.
- The e-safety coordinator 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, 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 videoconference call.
- Videoconferencing 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 Head Teacher .
- 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 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 is 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 e-safety team will monitor 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.
- Personal data files may be transferred on USB sticks only if the USB stick has been encrypted.

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 e-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.

Laptops

- Staff should store school laptops in a secure location overnight.
- If school laptops are taken home, staff are responsible for their security.
- School laptops 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 and no other person should tamper with them.

Portable Storage Devices

- If staff need to use a mobile storage device then it must be password protected.
- All users should ensure that data stored on mobile storage devices e.g. pen drives, disks, CD’s DVD’s have been downloaded using anti-virus software.
- All users are responsible for the security of mobile storage devices.
- Images of children should not be stored on mobile storage devices.
- Pupils are 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 e-Safety Issue

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 ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Reporting Procedures

Reporting Accidental Access to Inappropriate Material

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

1. Inform the e-Safety coordinator/team member of the incident and give the website address.
2. Log the web address, time and username in the e-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 e-Safety coordinator should contact the LA e-Safety contact for 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 of the Durham Net who accidentally comes across illegal material should do the following: -

1. Report the incident to the e-Safety coordinator/team member.
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.
4. Go to the IWF website at www.iwf.gov.uk and click the report button.
5. If reporting a URL do not use copy and paste, type the URL.

Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the regional broadband 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 Northern Grid to complete an internal investigation.
4. If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Northern Grid 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.
5. 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, Northern Grid or Easynet 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 co-ordinator and governors of the school, as deemed appropriate.

Key Contacts:

Mike Hamilton (LA e-Safety Contact for Schools) Tel: 0191 4272123 email: mike.hamilton@ictinschools.org

Authorising Access

Authorising access to the Internet and other ICT resources.

- All staff and pupils must read and sign an Acceptable Use Policy before using any school ICT 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 ICT 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 e-safety.

Communicating this Policy

Introducing the E-Safety Policy to Pupils

- A programme of training in e-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 school's Kidsafe tutors.
- E-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 KS1 and another when they move into KS2

Staff and the e-Safety Policy

- All staff will have access to the school e-safety policy via Google Drive and its importance explained. • 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 e-safety policy in newsletters, the school brochure, Class Dojo and on the school Website.
- The school will maintain a list of e-safety resources for parents/carers and share these via the school website and Class Dojo. School will also promote e-safety annually during e-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 e-Safety on an individual or group basis when needed. Parents are contacted if their child is involved in an e-safety issue.

Appendices

Legislation

Schools should be aware of the legislative framework under which this e-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 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 Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks 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, health professionals, connexions 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 teacher s, 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 2020

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.

Fellgate Primary School

Responsible Internet Use Agreement (KS1)

- I understand that school wants me to enjoy using the internet and other technologies to help my learning but I know that I must use them in a responsible way.
- I will keep my password secret.
- I will only use the internet when an adult is with me.
- I should only click the buttons and links when we know what they do.
- I will always tell an adult/teacher if something online makes me feel upset, unhappy, or worried.
- I will not do anything that will upset other children when I use the school's computer equipment or cameras.

Remote Learning

- If I need to learn online at home, I will also follow these school rules.
- Remote learning will only take place using Goggle Classroom, Class Dojo and Google Meet during usual school times.
- My use of Google Classroom, Class Dojo and Google Meet is monitored to help keep me safe.
- I will only use my school provided email accounts and login to access remote learning.
- I will not share my login/password with others
- I will not share any access links to remote learning sessions with others.
- When taking part in remote learning I will behave as I would in the classroom. This includes: using appropriate language, not taking or recording images/content without agreement from the teacher and/or those featured.
- When taking part in online learning I will: mute my video and microphone if requested by my teacher, wear appropriate clothing and be in a suitable location, ensure backgrounds of videos are neutral and personal information is not visible, attend lessons in a shared space or in a room with an open door where I can be supervised by a parent/carer or another appropriate adult.
- I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously.

Child's name:

I agree to these rules (signed):

Date:

Fellgate Primary School

Responsible Internet Use Agreement (KS2)

In our school the computers are installed with internet access to help learning. The rules below help us to be fair to others and keep everyone safe. Please read the rules with your child, sign and return to school.

- I understand that my teachers will help me know what is acceptable and unacceptable when using computers, the internet, mobile phones, email, online communities, digital cameras and other ICT and I will listen carefully to the advice I receive.
- I will ask permission before using the internet.
- I will not bring mobile phones into school, without the permission of the head-teacher.
- I will not use my own disks or pen drives in school without the teacher's permission.
- I know that when I use the internet I must only access the sites that my teacher approves and I will never try to access my personal email account, chat rooms or social networks in school.
- I will keep any passwords secret and not share them with others.
- I know that I should only access and delete my own work, with the teacher's permission.
- I know that all my communications with other people using ICT should be polite and friendly and will not deliberately send anything unfriendly or nasty.
- I understand that I must not give out any personal details, such as my name, address or phone number or arrange to meet anyone.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.
- I know that the school can check my computer files and the internet sites I visit and that if they have any concerns about my safety we will contact my parent/carer.
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

Remote Learning

- If I need to learn online at home, I will also follow these school rules.
- Remote learning will only take place using Goggle Classroom, Class Dojo and Google Meet during usual school times.
- My use of Google Classroom, Class Dojo and Google Meet is monitored to help keep me safe.
- Only members of Fellgate Primary School can access system name.
- I will only use my school provided email accounts and login to access remote learning.
- I will use privacy settings as agreed with my teacher.
- I will not share my login/password with others
- I will not share any access links to remote learning sessions with others.

- When taking part in remote learning I will behave as I would in the classroom. This includes: using appropriate language, not taking or recording images/content without agreement from the teacher and/or those featured.
- When taking part in online learning I will: mute my video and microphone if requested by my teacher, wear appropriate clothing and be in a suitable location, ensure backgrounds of videos are neutral and personal information is not visible, attend lessons in a shared space or in a room with an open door where I can be supervised by a parent/carer or another appropriate adult.
- I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously.

Child's name:

I agree to these rules (signed):

Date:

Pupil Consent form – Fellgate Primary School

Please place a tick in your desired option	Agree	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 within school publications (such as newsletters)		
Allow the use of photographs/videos on ClassDojo		
Allow use of photographs/videos for use on the school website		
Allow use of photographs/videos for use on school social media (such as Facebook, twitter)		
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)		
I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19.		
I will ensure my child's access to remote learning is appropriately supervised.		
When accessing video learning, I will ensure they are in an appropriate location (e.g. not in bed) and that they are suitably dressed.		

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.

Fellgate Primary School Acceptable Use Agreement for Staff

- I have read a copy of the school’s e-safety/acceptable use policy (available on the school network).
- I will only use the school email /internet/network for professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Board .
- I will only use the approved, secure email system for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will report any accidental access to inappropriate materials to the eSafety Coordinator/e-safety team.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school’s network security and confidentiality protocols.
- I will not connect a computer or laptop to the network/internet that does not have up to-date version of anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of pupils or colleagues without permission.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access email/internet/school network.
- I understand that all internet usage will be logged and this information could be made available to my manager on request.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any ‘significant personal use’ as defined by HM Revenue & Customs.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.
- I agree to follow the ‘remote learning guidelines’ outlined in this policy.

Name: **Job title:**

Signature: **Date:**

Fellgate Primary School Acceptable Use Agreement for Third Party Use

The school network provides internet access to third parties, people other than staff and students. This AUP will help protect third parties, students and the school by clearly stating what is acceptable and what is not.

- Access must only be made via the user’s authorised account and password, which must not be given to any other person.
- Storage media must not be brought into school unless permission has been given.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the user’s own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. email should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school computing systems may not be used for private business purposes, unless the Head teacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of the computing systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of internet access.

Please complete, sign and return to the school secretary:

I have read and understand the school's 'Acceptable Use Agreement'. I will use the computer system and internet in a responsible way and obey these rules at all times.

Name: **Signed:**

Address: **Date:**

October 2020

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 afterschool and so if your child must have a phone, we ask that you complete the form below.

As part of our e-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 ………………………………… (Childs 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……………………………………….(Childs signature)

Signed ……………………………………….. ……(Parent/Carer)

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	• Small number of named members of staff to have responsibility of posting to 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

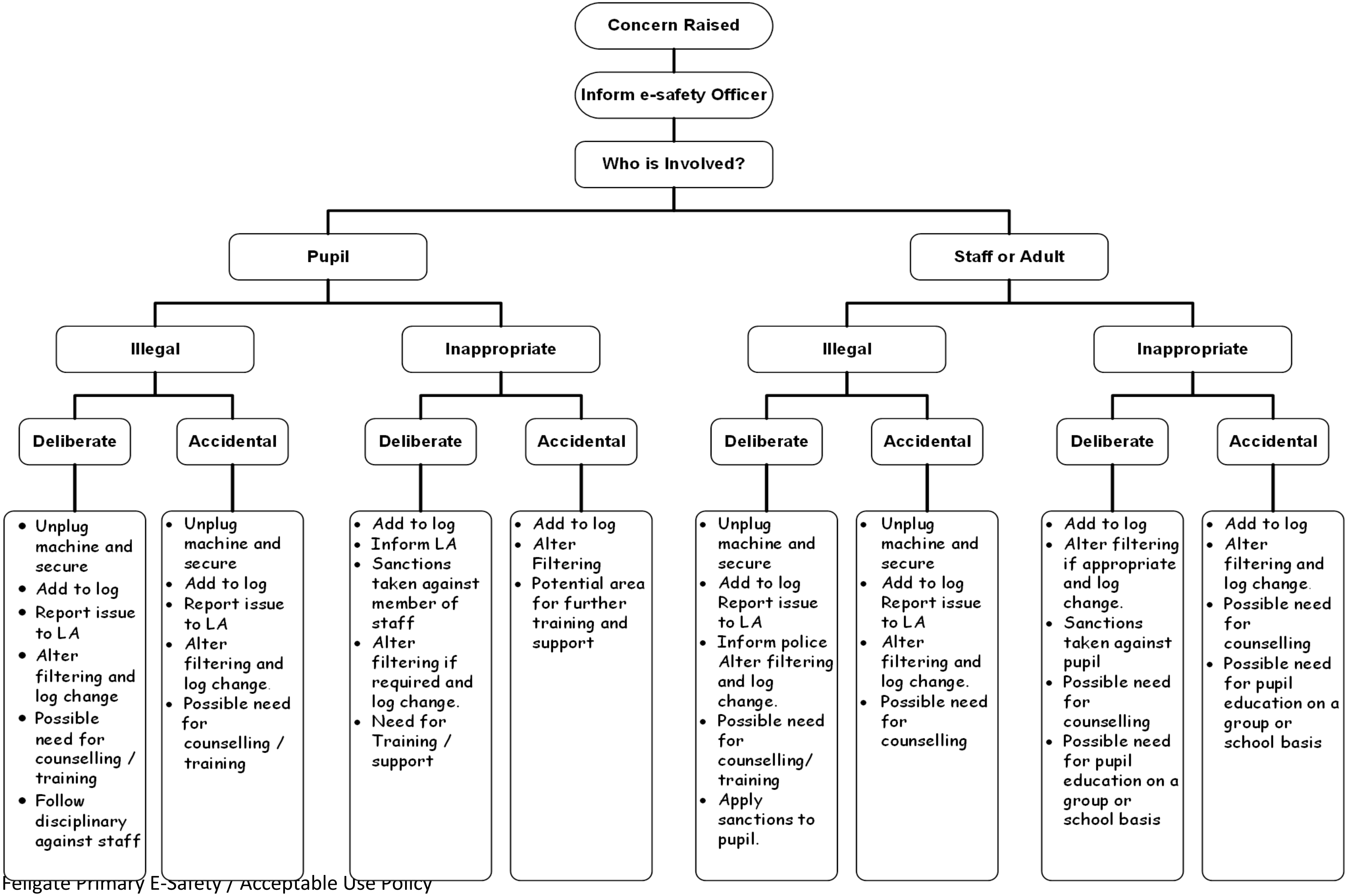
Harassment	All	• Encourage disclosure of any harassment. • Meet with affected parties if possible. • Ask for apologies and removal of posts. • Revision of AUP's for all stake holders. • Meet with Union representative if staff member is involved. • Contact police if situation is not resolved.	E Safety training and awareness for all stake holders.	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 to 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 log ins 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 such sites as Wayback machine.		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	Ensure virus checking software is enabled, up to	Low
Purchasing from applications	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 e-safety Incident



Concern Raised

Inform e-safety Officer

Who is Involved?

Pupil

Illegal

Deliberate

- Unplug machine and secure
- Add to log
- Report issue to LA
- Alter filtering and log change
- Possible need for counselling / training
- Follow disciplinary against staff

Accidental

- Unplug machine and secure
- Add to log
- Report issue to LA
- Alter filtering and log change.
- Possible need for counselling / training

Inappropriate

Deliberate

- Add to log
- Inform LA
- Sanctions taken against member of staff
- Alter filtering if required and log change.
- Need for Training / support

Accidental

- Add to log
- Alter Filtering
- Potential area for further training and support

Staff or Adult

Illegal

Deliberate

- Unplug machine and secure
- Add to log Report issue to LA
- Inform police Alter filtering and log change.
- Possible need for counselling/ training
- Apply sanctions to pupil.

Accidental

- Unplug machine and secure
- Add to log Report issue to LA
- Alter filtering and log change.
- Possible need for counselling

Inappropriate

Deliberate

- Add to log
- Alter filtering if appropriate and log change.
- Sanctions taken against pupil
- Possible need for counselling
- Possible need for pupil education on a group or school basis

Accidental

- Add to log
- Alter filtering and log change.
- Possible need for counselling
- Possible need for pupil education on a group or school basis