DIGITAL SYSTEMS & ONLINE SAFETY FRAMEWORK INCLUDING USE OF AI

1. Introduction

In an increasingly connected and technology-driven environment, our organisation relies on a wide range of digital tools, online platforms, and information systems to operate safely, efficiently, and collaboratively. To support this, it is essential that all staff, contractors, and relevant stakeholders understand their responsibilities when using digital resources and engaging in online environments.

This umbrella policy brings together a collection of our existing digital-related policies—such as those covering acceptable IT use, data protection, cybersecurity, social media activity, and online communication standards—into a single, coherent framework. Its purpose is to provide clarity, consistency, and ease of reference, ensuring that all digital and online practices across the organisation uphold our values, meet legal and regulatory requirements, and protect both individuals and organisational assets. Some policies are written specifically with Swinemoor Primary School's context in mind, and some are adopted from East Riding of Yorkshire Local Authority.

By consolidating these policies, we aim to create a unified approach that supports safe, responsible, and effective digital behaviour. This framework sets expectations for conduct, outlines the safeguards in place, and ensures that everyone engaging with our digital systems and online platforms does so with integrity, awareness, and accountability.

Links to other policies and practices

- Whistleblowing Policy
- Anti-bullying Policy
- Behaviour and discipline policy
- Child protection policy
- Code of conduct
- Complaints policy
- Data protection policy
- Use of images policy
- Mobile phone use policy (for pupils and staff)

2. Scope

This framework applies to:

- all teaching and non-teaching staff;
- pupils across EYFS, KS1 and KS2;
- parents and carers;
- governors and volunteers;
- external visitors using school equipment or platforms.

It covers the use of:

- school devices and networks, whether on site or remote;
- personal devices used for school purposes (where permitted);
- cloud platforms, learning systems, and communication tools;

- digital content, online behaviour, and communication;
- social media, websites, and digital publishing;
- data storage, sharing, and protection.

3. Roles & Responsibilities

Headteacher

- Ensures the implementation of all digital and online policies.
- Allocates resources for digital safeguarding and infrastructure.
- Supports staff training and ensures compliance.

Designated Safeguarding Lead (DSL)

- Oversees all online safety and digital safeguarding matters.
- Manages online safety incidents and referrals.
- Ensures staff and pupil education on safe digital practices.

Computing/ICT Lead

- Manages curriculum delivery of computing and digital literacy.
- Liaises with technical support providers.
- Ensures filtering/monitoring systems meet statutory standards.

Staff

- Follow all acceptable use requirements and related policies.
- Report digital concerns or incidents immediately.
- Model safe, responsible online behaviour.

Pupils

- Use devices and online platforms responsibly and respectfully.
- Report anything upsetting or unusual to a trusted adult.
- Follow their age-appropriate acceptable use requirements.

Parents/Carers

- Reinforce safe online behaviour at home.
- Follow parent acceptable use requirements.
- Work in partnership with school to ensure pupil safety.

Review Date: December 2028

CONTENTS

A) FILTERING AND MONITORING POLICY ……... 4 – 5

B) ACCEPTABLE USAGE POLICY …….. 6 – 9

C) PUPIL USAGE CHARTER …….. 10

D) SAFETY IN A DIGITAL WORLD: GUIDE FOR YOUNG PEOPLE……. 11 – 12

E) SAFETY IN A DIGITAL WORLD: GUIDE FOR PROFESSIONALS……. 13 – 14

F) ONLINE SAFETY POLICY…….…….. 15 – 24

G) ARTIFICIAL INTELLIGENCE POLICY…… 25 – 32

H) GUIDANCE ON THE USE OF SOCIAL MEDIA (LA ADOPTED)…….. 33 – 45

Filtering and Monitoring Policy

In accordance with *Keeping Children Safe in Education (KCSiE) 2023*, the school must implement appropriate filtering and monitoring to safeguard pupils from harmful or inappropriate online content. KCSiE requires that:

- The school's approach to online safety, including filtering and monitoring on school devices and networks, is reflected within the **Child Protection Policy**, taking into account pupil access to mobile phone networks.

- The **Designated Safeguarding Lead (DSL)** holds overall responsibility for the management and oversight of filtering and monitoring arrangements. The Lead Governor for Filtering and Monitoring is Mr S. Richardson.

- Governing bodies must consider:
    - the number and age range of pupils;
    - pupils who may be at increased risk of harm;
    - how frequently pupils access the school's IT systems.

- Schools must:
    - identify and assign clear roles and responsibilities for managing filtering and monitoring;
    - review filtering and monitoring provision at least annually;
    - ensure harmful and inappropriate content is blocked without creating unreasonable barriers to teaching and learning;
    - maintain effective monitoring strategies that meet the school's safeguarding requirements.

Local Authority Provision

The East Riding Local Authority provides the school's filtering and monitoring service via **Smoothwall**, managed through Local Authority firewalls and ER proxy settings.
Key principles include:

- Internet access permissions are configured by ER through tiered proxy settings, providing broader access for staff and more restricted access for pupils.
- SafeSearch is enabled across search engines, and HTTPS decrypt and inspect is used to filter explicit search terms.
- ER's Communications and Security Teams, including the specialist lead (Paul Foster), are trained directly by Smoothwall. Ongoing staff training is delivered in-house, with access to Smoothwall third-line support when required.
- The filtering system produces reports and automated alerts for breaches.
    - Daily reports are generated for any filtering violations.
    - Alerts concerning suicide or severe safeguarding risks generate **instant notifications** to the DSL and/or senior leaders, with additional notification from the Local Authority where possible.
- Devices with correct proxy settings are filtered according to assigned profiles (e.g., Key Stage, Staff, Network Administrator).
- Devices without the appropriate proxy settings are classed as **transparent devices**, placed under the highest filtering restrictions as their users cannot be identified. Physical recording logs are advised to maintain accountability for such devices.

School Arrangements (Swinemoor Primary School)

Swinemoor Primary School will implement the following measures to ensure that filtering and monitoring arrangements are effective, compliant, and robust:

- **Compliance with Local Authority systems**
  The school will use the Local Authority's Smoothwall filtering and monitoring service and will ensure that all filtering rules, proxy settings, and configuration requirements are applied consistently across devices and networks.
- **System maintenance and updates**
  The school will ensure that all filtering and monitoring systems remain up-to-date and will request technical support from the Local Authority where necessary.
- **Monitoring of alerts and reports**
  A nominated, responsible member of staff will receive, review, and action all notifications, alerts, and reports generated by the filtering and monitoring system.
    - At Swinemoor Primary School, the nominated staff member is **George McGowan**.
    - Alerts will be reviewed **daily**, with appropriate follow-up actions taken and logged.
- **Oversight and safeguarding integration**
  The DSL will oversee all filtering and monitoring arrangements and ensure that any concerns arising from system alerts are managed in accordance with the school's safeguarding procedures.
  Filtering and monitoring arrangements will be reviewed at least **annually** by the DSL, in consultation with technical support providers and the governing body.

Acceptable Usage Policy

This policy should be read in conjunction with the following guidance: Safety in a Digital World: Guide for Children and Young People.

Swinemoor Primary School will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used if parental consent has been given

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in for education, business and social interaction. The school has a duty to provide all students with quality Internet access as part of their learning experience.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.

How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-coordinator.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Whole-class or group e-mail addresses should be used.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- The headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Are newsgroups and chat safe?

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. The importance of chat room safety will be emphasized.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

How will Internet access be authorised?

- Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor ERYC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?

- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-coordinator.
- The Internet Service Provider also provides a system to filter unsuitable material. Any material which escapes the filter will be reported to the ISP immediately.

How will the policy be introduced to pupils?

- Pupils must accept the terms of the **Pupil's Acceptable Usage Charter** and **Safety in a Digital World: Guide for Children and Young People** before having access to digital devices or the internet.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will precede Internet access.

How will staff be consulted?

- All staff must accept the terms of the **Safety in a Digital World: Guide for Professionals** before using any internet resource in school.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is utilised.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal software may not be brought into school without specific permission and a virus check.

- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues

Swinemoor Primary School

Pupil's Acceptable Usage Charter

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- **I will ask permission before entering any Web site, unless my teacher has already approved that site.**
- **I will not look at or delete other people's files.**
- **I will not bring software into school without permission.**
- **I will only e-mail people whom my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will not use social media in school.**
- **I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I know that the school may check my computer files and may monitor the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

All personal data held on the school's network is subject to the Data Protection Act 1998 (and subsequently the General Data Protection Regulation (GDPR) and the school's Data Protection Policy.

Signed..... **Date.....**

Safety in a Digital World: Guide for Children and Young People

Digital technology opens up a world of entertainment, opportunity and knowledge. To help you stay safe this guide aims to provide information on:

- The benefits of Digital Technology
- Addressing the risks
- Further advice and support

The safety advice below applies to all digital technology including computers, mobile phones, TVs, iPods, mass storage devices *etc*.

The Benefits of Digital Technology
You can use digital technology for many reasons, including:
Finding and sharing information – Researching topics on the internet, for school, college and for personal interests, and sharing media like files, pictures, films and music.
Keeping in touch with family and friends – Staying in touch with family and friends through: Email, Instant Messaging (IM), Social Networking and chat rooms technology can be useful for contacting people in an emergency and making new friends in a safe way.
Entertainment – Listening to music, watching films, and playing interactive games.
Shopping – Buying items from companies and individuals all over the world, including online auctions.

Addressing the risks: Digital technology agreement:
There are however some risks in using digital technology – follow this advice and sign this agreement to help keep you safe.

I agree to keep my personal information safe

Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings. This can help keep you safe.
Don't give out personal information like email addresses, home or school addresses or mobile phone numbers to people you do not know.
Only post photographs which you would be happy with your parents/carers seeing and make sure they don't show addresses. Photographs you post can be copied and sent to other people meaning you are not in control of them.

I will tell adults about the sites that I am worried about.

I agree not to meet people without asking a parent/carer/adult.

Some people on the internet are not who they say they are. Be careful who you chat to and make friends with on Social Networking sites like Facebook, Instagram and Snapchat. Never agree to meet someone without letting an adult know.

I agree to report and worries I have to an adult.

If anyone online makes you worried or says things that make you feel uncomfortable tell an adult or click 'Report abuse' button (some websites will ask you to download this first) and block them.
Do not respond to upsetting messages and cyber-bullying. Keep the message and show it to an adult you trust.

I agree not to use digital technology to bully people or make threats.

Cyberbullying is not acceptable and can cause distress.
Treat people as they would like to be treated.

Signed..... **Date.....**

Further advice and support:
If you want to find out more about using digital technology safely go to:
www.thinkyouknow.co.uk Digital safety advice
www.ceop.gov.uk Report Abuse Button

Remember the internet safety code. Click Clever, Click Safe

- **Zip It** – Keep your personal stuff private and think about what you say and do online .
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.

Safety in a Digital World: Guide for Professionals

Technology is provided and maintained for the benefit of all staff within Swinemoor Primary School to enhance skills and become more effective in the workplace. You are encouraged to use and enjoy these resources, using the following agreement as a guide.

There is a need to ensure that digital technologies are used appropriately and for you to have an understanding of your responsibilities in keeping yourself and young people safe. This guide aims to assist you, making sure that you have all necessary measures in place.

Internet and Email

- **I agree to only access suitable material**;
  I am aware that accessing materials which are unlawful, obscene or abusive is not permitted.
- **I agree to report unsuitable material;**
  If I receive an email containing material of a violent, dangerous, racist, or inappropriate content, I will always report such messages to the E-safety Co-ordinator.
- **I agree to the professional code of behaviour;**
  I appreciate that other users might have different views from my own and acknowledge that the use of strong language or aggressive behaviour is not acceptable.
- **I agree to keep within copyright laws;**
  I will respect work and ownership rights of people, including abiding by copyright laws.
- **I agree to the responsible use of social networks, both within and outside the workplace;**
  The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.

Equipment

- **I agree to take care to protect hardware and software;**
  This includes protecting the ICT equipment from spillages by eating or drinking well away from them. I will always get permission before installing, attempting to install or storing programs of any type on the ICT equipment. I will always check files brought in on removable media (such as CDs, flash drives *etc*) and mobile equipment (*e.g.,* laptops, PDAs *etc*) with antivirus software and only use them if they are found to be clean of viruses. I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could damage files or software.
- **I agree to only using equipment within the context of my professional role;**
  I will only use ICT equipment for Swinemoor Primary School purposes. I understand that activities such as buying or selling goods are inappropriate.

Security and Privacy

- **I agree to take measures to protect access to data;**
  I will keep my log-on user name and password private, **always log off when I have finished working or am leaving the ICT equipment unattended**. I am aware that I must never use someone else's user name. To protect myself and the systems, I will respect the security on the ICT equipment; I understand that attempting to bypass or

alter the settings may put my work or other people's information at risk. I will not send sensitive information via FAX or non-secure email.

Mobile phones

- **I agree to always abide by Swinemoor Primary School policy for use of mobiles in the workplace;**
  I understand that the use of mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of the Headteacher and recorded.

Name
(print)……Signed……..……

Date ……..……

Online Safety Policy

Policy Overview

The purpose of this policy is to safeguard and protect all members of Swinemoor Primary School's online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of Swinemoor Primary School. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of the school's digital technology systems, both internally and externally.

Introduction

Online safety in schools is of paramount importance. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

School staff and governors play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can.

This policy is applicable to all members of Swinemoor Primary School. This includes, staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of the school's digital technology systems, both internally and externally within the home and community setting.

Online Safety School Statement

Swinemoor Primary School asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.

Swinemoor Primary School believes that the internet and associated devices are an integral part of everyday life.

Swinemoor Primary School affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.

Policy Scope

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports schools in meeting statutory requirements as per the DfE guidance under KCSiE (2021), Working Together to Safeguard Children (2018) and non-statutory guidance, Teaching Online Safety in Schools (2019). Effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of the safeguarding agenda.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, all staff must foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone's responsibility.

Defining online abuse: "*Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones"* (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

This policy should be read alongside the relevant policies relating to safeguarding of children and in addition to associated statutory legislation and guidance.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within Swinemoor Primary School

Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; headteacher, teachers, substitute teachers, work-experience staff, office staff, nurses, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Model good practice when using technology.
- Know the process for making referrals and reporting concerns.
- Know how to recognise, respond and report signs of online abuse and harm.
- Receive appropriate child protection training.
- Always act in the best interests of the child.
- Be responsible for their own continuing professional development in online safety.

Governors and Senior Leadership Team

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Carrying out risk assessments on effectiveness of filtering systems.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (Deputy DSL)

With respect to online safety, it is the responsibility of the DSL to:

- Ensure children and young people are being appropriately taught about and know how to use the internet responsibly.
- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.

- Take responsibility for all safeguarding matters, including online safety.
- Collaborate with the senior leadership team, the online safety lead and computing lead.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.
- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety.

Children and Young People

With respect to online safety in your school, children need to:

- Know who the DSL is.
- Engage in age appropriate online safety education opportunities.
- Contribute to policy development and review.
- Read and adhere to online safety policies.
- Respect the feelings of others, both off and online.
- Take responsibility for keeping themselves and others safe online.
- Where and how to find help with any online incidents or concerns.
- How, when and where to report concerns and when to seek help from a trusted adult.

The UKCCIS 'Education for a Connected World' framework aims to equip children and young people for digital life. It covers:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

Parents and Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Read and adhere to all relevant policies.
- Be responsible when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Support online safety approaches and education provision.
- Be a role model for safe and appropriate behaviour.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse.

Education and Training

Safeguarding activity across the United Kingdom (UK) continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of children and young people relies upon constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse or harm.

Online safety has a high emphasis on a competent well-established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall under one of three categories:

Contact: Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

Learners

Swinemoor Primary School will promote safe and responsible internet use:

- Education regarding safe and responsible use and access of the internet.
- Include online safety in Personal, Social, Health and Economic (PSHE) education, Relationships and Sex Education (RSE) and Information Computer Technology studies.
- Reinforce online safety messages as a continuum.

Swinemoor Primary School will support learner's understanding based on age and ability:

- Acceptable use posters in all rooms with internet access.
- Informing all learners of monitoring and filtering in place.
- Implement peer education strategies.
- Provide continuous training and education as part of their transition across key stages.
- Use alternative, complementary support where needed.
- Seeking learner voice.

Vulnerable Learners

Vulnerable children who need our help the most are not only missing out on opportunities to flourish online but are often experiencing the very worst that the online world can be. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

Swinemoor Primary School recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Swinemoor Primary School will ensure the effective and safe provision of tailored online safety education.
Swinemoor Primary School will obtain input and advice from specialist staff as deemed necessary.

Staff

Swinemoor Primary School will:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Provide up to date online safety training at least annually or more in line with legislative and statutory changes and/or online safety incidents arising.
- Ensure training will include recognition of risks and responding to concerns.
- Inform of monitoring and filtering processes.
- Make staff aware that their online conduct outside of work can impact upon their professional role and responsibilities.
- Advise of appropriate resources.
- Ensure that all staff are aware of procedures to follow in recognising, responding and reporting online safety concerns.

Parents and carers

Swinemoor Primary School will:

- Recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people.
- Ensure provision of resources, support and advice.
- Ensure provision and adherence to online safety policies and other policies of relevance.
- Advise of how and when to raise concerns.
- Provide details of all relevant contacts (for example, the DSL).

Cultivating a safe environment

"All staff should be aware of indicators, which may signal that children are at risk from, or are involved with serious violent crime. These may include increased absence from school, a change in friendships or relationships with older individuals or groups, a significant decline in performance, signs of self-harm or a significant change in well-being, or signs of assault or unexplained injuries. Unexplained gifts or new possessions could also indicate that children have been approached by, or are involved with, individuals associated with criminal networks or gangs" (DfE, 2019).

Children should be educated in an age-appropriate way around:

- ✓ How to evaluate what they see online
- ✓ How to recognise techniques for persuasion
- ✓ Their online behaviour
- ✓ How to identify online risks
- ✓ How and when to seek support

Evaluate: **How to evaluate what they see online**

This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Swinemoor Primary School will help pupils to consider questions including:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?

Recognise: How to recognise techniques used for persuasion

This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. A strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

Swinemoor Primary School will help pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation).
- Techniques that companies use to persuade people to buy something.
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design)
- Criminal activities such as grooming.

Online Behaviour

This will enable pupils to understand what acceptable and unacceptable online behaviour looks like. Swinemoor Primary School will teach pupils that the same standard of behaviour and honesty applies online and offline, including the importance of respect for others. Swinemoor Primary School will also teach pupils to recognise unacceptable behaviour in others.

Swinemoor Primary School will help pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online. For example, how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do.
- Looking at how online emotions can be intensified resulting in mob mentality.
- Teaching techniques (relevant on and offline) to defuse or calm arguments (for example, a disagreement with friends) and disengage from unwanted contact or content online; and
- Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

Identify: How to identity online risks

This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

Swinemoor Primary School will help pupils to identify and manage risk by:

- Discussing the ways in which someone may put themselves at risk online.
- Discussing risks posed by another person's online behaviour.
- Discussing when risk taking can be positive and negative.
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations; i.e. how past online behaviours could impact on their future when applying for a place at university or a job for example.
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with.
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support

This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Swinemoor Primary School will help pupils by:

- Helping them to identify who trusted adults are.

- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations, such as Childline and the Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education).
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Responding to Online Safety Concerns

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for *[school name]* includes procedures to follow regarding online safety concerns.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies as per *[school name]* local process.
- Always adhere to local safeguarding procedures and report to the DSL or Deputy DSL.

Responding to Complaints

There are a number of sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer
- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk is in need of protection or services.
- Consideration by an employer of disciplinary action in respect of the individual (including suspension).

It is also the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL and Head Teacher (if DSL is not the Head Teacher).

Disclaimer

Whilst every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance, where errors are brought to our attention, we will correct them as soon as is practicable.

Artificial Intelligence (AI) Policy

This policy outlines how Artificial Intelligence (AI) is currently managed, restricted, and monitored at Swinemoor Primary School to ensure safe, ethical, and compliant use in line with Department for Education (DfE), Ofsted, and Information Commissioner's Office (ICO) guidance.

This policy applies to:

- All staff (teaching and non-teaching)
- Governors
- Contractors and third-party providers
- Pupils (by reference and restriction)

Current Position on AI Use in School

- Pupils do not have direct access to any AI tools in school.
- Google Search is the only currently approved tool pupils can use under supervised conditions.
- Use of open source generative AI may be used for curriculum and administrative purposes. Any AI software used must be transparent, explainable, robust and secure.
- Leaders will support staff to be aware of and comply with the DfE guidance for AI use 'Generative Artificial Intelligence in Education' policy paper.
- Use of AI must always comply with safeguarding and data protection requirements.

Acceptable Use by Staff

Staff may use AI tools (e.g. ChatGPT) for the following purposes:

- Curriculum resource development
- Drafting letters or communications (with human oversight)
- Administrative efficiencies (e.g. planning templates, summarising content)

Current AI tools that are appropriate may include but are not limited to: Chat GPT, Microsoft Copilot, Twinkl, Aila (Oak Academy Trust), Third Space Learning

Conditions for Use:

Large Language Models (LLMs):
Large Language Models are a type of artificial intelligence designed to understand and produce human language. These tools, such as ChatGPT, are trained on large amounts of text from books, websites, and other sources to learn how language works. They can be used to help students generate ideas, improve writing, or answer questions, but they do not "think" like humans and can sometimes provide incorrect or biased information. Their use should support learning and not replace students' own thinking or effort.

Machine Learning Principles:
Machine learning is a method that allows computers to learn from data and make predictions or decisions without being directly programmed for every task. It is the foundation behind many AI tools, including LLMs. Understanding that these systems learn patterns from past data helps us recognize their strengths and limitations. In a school setting, AI tools based on machine learning should be used responsibly, with an emphasis on critical thinking, ethical use, and awareness of data privacy.

Therefore:

- No personal data (of pupils, parents, staff, or any identifiable individual) is to be entered into any AI system.
- Only public figures already named in our published curriculum may be referenced when using AI.
- Any content generated by AI must be reviewed and approved by the user before use or dissemination.
- No automated decision-making is permitted — all outputs must be subject to human judgment.

Safeguarding and Online Safety

All AI use must align with the school's safeguarding, online safety, and acceptable use policies.
Pupils are not permitted to interact with generative AI systems (e.g. ChatGPT, Bard, Copilot).
Filtering and monitoring systems are in place to prevent unauthorised access to AI platforms.
Teachers must supervise any search engine use and ensure age-appropriate content filters are active.

Data Protection and Privacy

In accordance with the ICO's guidance:

- No personal or sensitive data may be shared with AI platforms.
- Staff must not use AI tools to process any pupil or staff data.
- Any use of AI involving data must be pre-approved by the school's Data Protection Officer (DPO). A Data Protection Impact Assessment (DPIA) has been carried out – **Appendix 1.**

Roles and Responsibilities

Headteacher / Senior Leadership Team (SLT):

- Ensure this policy is implemented and reviewed annually. The use and management of AI is fast paced and must be reviewed regularly.
- Approve any further AI tools for staff use following risk assessment and due diligence.
- Communicate to parents about the use of AI in school – **Appendix 2.**

All Staff:

- Comply with this policy in all instances of AI use.
- Report any misuse or concerns to SLT or the Designated Safeguarding Lead (DSL).

ICT Lead / DPO:

- Monitor AI-related risks and recommend updates to policy or practice.
- Support staff with technical queries or impact assessments.

Breaches of Policy

Any breach of this policy, including the unauthorised use of AI or inappropriate data handling, will be treated seriously and may lead to disciplinary action in line with the school's Code of Conduct.

Monitoring and Review

This policy has been created in line with guidance from the ICO and Ofsted - **Appendix 3**. Swinemoor Primary School recognise that the use and management of AI is fast paced and rapidly changing. This policy will be reviewed annually or sooner if significant changes occur in:

National guidance from the DfE, Ofsted, or ICO
AI technology or platforms in use at the school
Legal or safeguarding requirements

Appendix 1: Artifical Intelligence Policy

Data Protection Impact Assessment (DPIA)

Project/Processing Name: Use of AI Tools (ChatGPT) by Staff
School: Swinemoor Primary School
Date: 12th May 2025
Assessed by: Corina Boughton
Role: School Business Manager
Review Date: May 2026 or sooner, if required.

Purpose of the Processing

Staff at Swinemoor Primary School may use ChatGPT (a generative AI tool) to support:
- Lesson planning
- Curriculum resource development
- Drafting non-personal administrative text (e.g., letters, summaries)
- CPD-related research or teaching ideas

No decisions about individuals are made by AI. This tool is not used by pupils.

Nature of the Processing

- Type of processing: Text input and output generation
- Tool used: ChatGPT (OpenAI)
- Access: Staff-only, under strict internal policy
- Data types entered: None that qualify as personal data under UK GDPR. Staff must not enter pupil, staff, or parent data.
- Safeguards: Staff training, written AI policy, monitoring of AI use, filtering systems in place

Scope and Context

- Number of data subjects affected: None directly, as personal data is not processed
- System access: Limited to authenticated staff; no integration with school MIS or pupil systems
- Tool review: Approved by SLT; no other AI tools are currently permitted

Assessment of Necessity and Proportionality

Is the processing necessary? Yes, to support efficient lesson preparation and reduce admin burden
Is there a less intrusive method? Not applicable, as no personal data is processed
Is it proportionate to the aims? Yes — restricted, guided use within tight policy limits

Assessment of Risks and Mitigation

Risk	Likelihood	Impact	Mitigation Measures
Staff inadvertently enter personal data	Low	Medium	Policy explicitly prohibits this; regular staff reminders
Tool use expands without oversight	Medium	Medium	SLT to approve any new AI tools or expanded use
Data leakage via ChatGPT	Low	Medium	No sensitive data entered; usage monitored
Misuse or over-reliance on AI-generated content	Low	Low	Human oversight mandated; no AI-led decision-making

Consultation Process

Internal consultation with:
- Headteacher
- Senior Leadership Team (SLT)
- Data Protection Officer

ICO Criteria Check (High-Risk Flags)

According to the ICO's DPIA guidance, this project does not involve:
- Automated decision-making affecting individuals
- Processing of special category data
- Large-scale monitoring or profiling

Therefore, prior consultation with the ICO is not required.

Sign-Off

Name: [Insert Name] | Role: Headteacher / SLT | Signature: _____ | Date: _____
Name: [Insert Name] | Role: Data Protection Officer | Signature: _____ | Date: _____

DPIA Outcome Summary

This DPIA concludes that the staff-only use of ChatGPT, under strict controls and without processing personal data, presents minimal data protection risk. Swinemoor Primary School is compliant with UK GDPR and ICO expectations as long as current usage boundaries are maintained.

Appendix 2: Artifical Intelligence Policy

Dear Parents and Carers,

Responsible Use of Artificial Intelligence (AI) in School
As part of our commitment to providing a safe education at Swinemoor Primary School, we want to keep you informed about how we are approaching the use of Artificial Intelligence (AI) in our school. AI is becoming more common in education and everyday life. While there are exciting opportunities, it is vital that schools use these tools responsibly and with clear safeguards in place.

Children do not have access to AI tools like ChatGPT or other generative AI systems in school. Google search is the only AI-enabled tool children may use, and it is supervised and filtered for age-appropriate content.

At this time, ChatGPT is the only AI tool approved for staff use, and only for professional tasks such as drafting teaching resources or communications. **No personal data about pupils, parents, or staff is ever entered into any AI tool.** The only individuals mentioned in AI tools are public figures already included in our published curriculum.

We are following national guidance from the Department for Education, Ofsted, and the Information Commissioner's Office. Our focus is on safety, privacy, and using technology in a way that supports, not replaces - high-quality teaching.

As AI develops, we will continue to review our policy regularly. Any future changes will be carefully risk-assessed, and we will keep you fully informed.

If you have any questions or concerns about our approach to AI, please don't hesitate to contact the school office.

Yours sincerely,

Mr. L. A. Myers

Appendix 3: Artificial Intelligence Policy

What do the ICO and Ofsted say about the use of AI in schools?

Both the Information Commissioner's Office (ICO) and Ofsted have provided guidance on the use of artificial intelligence (AI) in UK primary schools, focusing on data protection, ethical considerations, and educational outcomes.

Information Commissioner's Office (ICO) Guidance

The ICO emphasizes that AI systems in schools must comply with UK General Data Protection Regulation (UK GDPR). Key points include:

1. Lawfulness and Transparency

- Schools must have a clear legal basis for processing personal data with AI, such as consent or legitimate interests.
- They should be transparent about AI usage, informing stakeholders about how personal data is processed.

2. Fairness and Bias Mitigation

- AI systems should be designed to avoid bias and discrimination.
- Schools must assess and mitigate potential biases in AI algorithms to ensure fair treatment of all students.

3. Data Minimization and Security

- Only necessary personal data should be collected and processed by AI systems.
- Robust security measures must be in place to protect data from unauthorised access or breaches.

4. Automated Decision-Making

- If AI systems make decisions that significantly affect individuals, schools must ensure human oversight and the ability for individuals to challenge decisions.

Ofsted's Position on AI in Education

Ofsted supports the use of AI in schools when it enhances educational outcomes and efficiency. Their approach includes:

1. Inspection Considerations

- Ofsted evaluates the impact of AI on teaching quality, learning outcomes, and safeguarding during inspections.
- They do not assess the technical quality of AI tools but focus on their application within the educational context.

2. Regulatory Principles

Schools are expected to adhere to principles such as:

- **Safety and Robustness**: Ensuring AI tools are secure and reliable.
- **Transparency**: Being open about how AI is used and how decisions are made.
- **Fairness**: Preventing discriminatory practices through AI.
- **Accountability**: Assigning clear responsibility for AI use and outcomes.

- **Contestability**: Allowing decisions made by AI to be challenged and reviewed.

3. Ongoing Research
Ofsted is conducting research to understand how schools use AI, aiming to identify best practices and potential risks. Findings are expected to inform future guidance and policy.

Summary
In summary, the ICO focuses on ensuring that AI use in schools complies with data protection laws, emphasising transparency, fairness, and security. Ofsted, on the other hand, assesses the educational impact of AI, encouraging its use to enhance learning while ensuring it aligns with regulatory principles and does not compromise educational quality or student welfare.

Guidance on the use of Social Media

EAST RIDING OF YORKSHIRE COUNCIL

Lead Directorate and Service:	Corporate Resources - People Services
Effective Date:	April 2019
Contact Officer/Number:	Employment Services Advice Centre (01482) 391221
Approved by:	CMT: 25.3.19, Min: 18681

Contents

Guidance on the use of Social Media 1

1. Scope 1
2. Background 1
3. Definitions 1
4. Statement 1
5. Corporate Requirements 2
6. Development including Consultation 2
7. Links with other Policies 2
8. Using Social Media 2
9. Responsibilities of Managers 3
10. Responsibilities of Employees 4
11. Bullying/Harassment on Social Media 6
12. References 8

Social Media Guidance Q and A 9

Guidance on the use of Social Media

1. Scope

This guidance applies to all employees of the Council including school-based employees where it has been adopted by the respective school governing body.

The guidance also applies to contractors, agency workers, volunteers, those on apprenticeships and student/work placements, any third party, working on behalf of the Council.

The policy applies to the use of social media for both business and personal purposes, whether during or outside of office hours, and whether Council ICT facilities or the individual's personal equipment is used.

However, the guidance cannot cover all eventualities and employees should consult their Line Manager if they are in any way unsure about what is and is not acceptable use of social media. An on-a-page version of the guidance can be found in Appendix A.

2. Background

The Council supports employees' use of the internet, as detailed in the Policy and Guidelines on the Use of the Internet. This guidance provides advice for Managers and employees in the use of social media, both for personal and, where permitted, professional use.

The popularity of social media over recent years opens up new opportunities for contact and communication. With these opportunities there are however pitfalls which give rise for the need to ensure robust procedures and governance are in place to minimise the risk to the Council and its employees. While recognising the need to have procedures and governance in place, the Council aims to be a modern employer, with a modern workforce in a modern workplace, and aligned to that is the principle that staff are trusted to have access to social media and are trusted to be responsible and professional with that access.

3. Definitions

'Social media' is the term commonly given to websites and online tools which allow users to generate their own media and interact with each other in some way - by sharing information, opinions, knowledge and interests. As the name implies, social media involves the building of communities or networks, encouraging participation and engagement.

Social media includes, but is not limited to, blogs; wikis; social networking sites such as Facebook and LinkedIn; micro blogs such as Twitter; photo sharing sites such as Instagram, and Flickr; messaging apps such as Snapchat and WhatsApp, and video sharing sites such as YouTube.

There are many more examples of social media than can be listed and it is a constantly changing area. The policy refers to the examples listed and any new social media which is developed in the future.

For convenience this guidance will use the term 'social media' throughout. All employees should understand that any information shared through social media, even if done so within a personal capacity, may be subject to Council policies, copyright, data protection and other legislation.

4. Statement

Explaining what we do, how we do it, and why we do it is already embedded in how we communicate with residents and visitors. Social media by its very nature adds a further level of transparency and accountability to the public.

Social media allows residents and customers to input into decisions, to challenge them and for replies to be broadcast to many rather than to one individual. Organisations can hear direct from those affected by decisions, the positive and negative, and explain and/or defend decisions in response to questions or concerns raised.

This guidance applies to online participation in social media, in both a personal and a professional capacity, and sets out the standards of behaviour expected as an employee of the Council.

5. Corporate Requirements

- Growing the Economy.
- Helping Children and Young People Achieve.
- Promoting Healthy Lifestyles.
- Protecting the Vulnerable.
- Valuing the Environment.

6. Development including Consultation

This guidance has been developed in conjunction with the following teams:

- Customer Strategy and Development
- Corporate Communications
- People Services
- Legal and Democratic Services
- ICT

7. Links with other Policies

The Council expects the highest standards of behaviour from its employees and staff should apply the same standards of conduct online as they are expected to apply offline. Misuse of social media is taken very seriously. Any misuse can result in action being taken under the Council's Disciplinary Policy which can result in dismissal. It is important that employees are aware that posting information on social networking sites, in a personal capacity cannot be isolated from their working life, even if the employee is using their personal social media account in their own time. Any information published online can be accessed around the world within seconds and will be publicly available for all to see.

Employees must know and adhere to the following Council policies:

- Policy and Guidelines on the Use of the Internet (Q1).
- Policy and Guidelines on the Use of Electronic Mail (Q2).
- Disciplinary Policy and Procedure (G1).
- Code of Conduct for Employees (G4).
- Harassment/ Bullying Policy and Procedure (O2).
- Equality in Employment Policy and Guidelines (O1).
- RIPA Policy.
- Non-RIPA Procedure (G2).
- Any other Council policies considered applicable.

Employees should consult their Manager in the first instance should they have any queries regarding the above policies or guidance.

8. Using Social Media

Access to social media from the corporate network is permitted as a business tool during working time. When a login is required, access is only allowed using a work social media account. Employees

must not access social media for work purposes using their personal accounts, with the exception of professional networking sites such as LinkedIn. (Please see below which explains how to set up a work social media account.)

Employees can access social media for personal use during their own time, ie before or after their working start and finish time or in their lunch break. An employee's work pattern as entered onto iTrent will be the definitive record for defining an employee's work/non work pattern. Please refer to the Council's Policy and Guidelines on the Use of the Internet for more information.

If employees require a work account, permission must be sought and supported by the employee's Line Manager. Managers must agree in advance the scope, context and timings of social media work accounts. When applying employees need to state which platforms they require work accounts for, clearly detailing the reason why the work account is required. Access to the social media work account request e-form is accessed via the social media section of the intranet, at http://insight.eastriding.gov.uk/socialmedia.

The work account must clearly show the employees name, job title and feature the Council logo, where possible, so it is clear that any activity being undertaken on social media is being undertaken on behalf of the Council. The account will also refer customers to corporate accounts for any service-related enquiries and be set up using the employees work email address. This account must not be used for personal use.

Under no circumstances should log-ins or passwords be shared. The corporate ICT Security Policy forbids the sharing of passwords by Council employees, and strongly advises against the sharing of any passwords with any third party. Furthermore, the sharing of passwords does not accord with the Data Protection Act 2018 and the General Data Protection Regulations 2018.

Members of the public have access to social media and can access the personal accounts of employees. Employees are encouraged to set up appropriate privacy settings to avoid personal information being accessed. Any complaint relating to activity on social media will be investigated fully in line with the Council's policy and procedures.

The Council takes bullying and harassment seriously, and incidents of this nature occurring on social media are no less serious. Reports of cyberbullying will be investigated in line with the Harassment and Bullying Policy, and may lead to disciplinary action being taken, up to and including dismissal.

9. Responsibilities of Managers

Managers have a responsibility to ensure access to social media is not abused. Managers are best placed to monitor access to social media during work time to ensure this is used solely as a business tool and ensure access for personal use only takes place during the employees own time.

Concerns about impartiality, confidentiality, conflicts of interest or commercial sensitivity should be borne in mind.

Managers should be aware that social media may provide a platform for harassment and bullying. Complaints of this nature should be taken seriously and fully investigated in line with Council policy and procedure.

Managers have a responsibility to ensure employees are clear on their responsibilities under these guidelines. If

any employee requests guidance on the use of social media and the Manager is unsure they should seek advice from the Principal Marketing Officer.

10. Responsibilities of Employees

This guidance applies to employee's online participation for both professional and personal reasons and sets out the standards of behaviour expected as an employee of the Council. Employees should participate on social media in the same way as they would with other media or public forums, such as giving presentations. All employees are expected to behave appropriately and responsibly and should be aware that they may be accountable to the Council for actions outside of their work. Any item on the internet is considered to be legally published and available to all without restriction.

It is the responsibility of employees to ensure that their use of social media whether in a professional or a personal capacity is in accordance with this guidance and other relevant Council policies. Social media can blur the lines between our professional and personal lives, so employees must ensure their behaviour on social media does not impact negatively on the Council's reputation. Any use of social media that amounts to a breach of this guidance could result in action being taken under the Council's Disciplinary Policy and Procedure.

Individuals working for the Council are bound by a duty of confidentiality to protect the information they have access to during the course of their work. Disclosure of confidential information on social media, or by any other means, is a breach of the Council's Code of Conduct for employees and, in certain circumstances, may also breach the Council's Data Protection Policy and the General Data Protection Regulations 2018.

Social media may be used as a platform for bullying behaviour. Whether in their personal or professional capacity, employees should not utilise social media

to discriminate, make offensive or inappropriate comments about a colleague, customer or the Council or any outside parties with whom the Council conducts its business or otherwise undertake acts that could be interpreted as harassment or bullying of others. Reports of harassment or bullying will be investigated fully and may lead to further action being taken under Council's Disciplinary Policy and Procedure.

Employees should be aware that if they break the law in their use of social media, (for example by posting something defamatory), they will be personally responsible. The Council may also be held responsible for the acts of its employees.

It is not advisable for employees to invite customers/clients to become their friends on personal social networking sites (with the exception of professional networking sites such as LinkedIn) as there may be a conflict of interest or security and privacy issues. The Code of Conduct for employees makes it clear that close personal familiarity between employees and elected members is to be avoided, therefore employees should not invite elected members to be their friends on their personal social networking sites nor should they accept invitations from them to be their friend or make postings on their blog. A separate guidance document has been produced for members.

For a work social media account it may be that the objectives of the employee includes creating a network of 'friends' and/or followers which may include members or potential suppliers. All activity on social media should remain professional at all times in order to avoid any conflict with the Code of Conduct for Employees.

The corporate social media sites enable the Council to engage in a cost-effective way with its citizens. In order to limit reputational risk employees should not make negative comments about the Council on social media sites nor bring any grievances to the Council's attention via social media. Reports of negativity online will be investigated fully and may lead to further action being taken under Council's Disciplinary Policy and Procedure.

If employees have access to work related sites such as knowledge sharing hubs and forums, or they have access to social media in a professional capacity, they are responsible for understanding what purpose they are accessing social media and the standard of behaviour expected.

Employees who access customer, client or employee social media accounts as part of their duties are required to comply with the Council's Regulation of Investigatory Powers Act 2000 (RIPA) Policy and non-RIPA Procedure, as appropriate. Employees should seek additional guidance from their Line Manager and legal services where appropriate.

Forums often have open access with limited security. Information that is shared by employees either as an individual or as an employee of the Council can be used by others to manipulate to the detriment of the employee or the Council. Employees should always take this into consideration before they share information.

Employees need to be aware that information they post on their personal or work social media profile can make them identifiable to service users, as well as people they know in a private capacity, and this can adversely impact on themselves and the Council.

An employee's personal social media account should not, directly or indirectly, give the impression that they are endorsed by, or speaking on behalf of the Council. It is important however that employees are aware that posting information on social networking sites in a personal capacity cannot be entirely isolated from their working life.

Anything published on an employee's work social media account will give the impression that they are endorsed by, or speaking on behalf of, the Council. It is important that employees posting any information relating to Council services ensure that the information is correct as they will be representing the Council.

Employees should be clear that online sites such as Facebook are in the public domain and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Employees who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard. Nothing posted on social media is ever truly private and may be impossible to delete/withdraw once published.

11. Bullying/Harassment on Social Media

Employees can sometimes find themselves the subject of criticism, abuse or threats on social media from colleagues, the public or members. Such comments or threats, from whatever source, can have a debilitating effect on the employee and leave them feeling isolated and vulnerable.

Depending on the source of the abuse there may be a limit to the action that the Council or an employee can take with regard to such attacks, however, this guidance is intended to provide employees with a range of tools to deal with such harassment as well as setting out the support that can be provided by the Council to employees suffering such abuse.

General Principles

Employees are advised to:

- Not respond to bullying and harassment on social media either on personal or work accounts - this may escalate the abuse.

- Discuss the comments with their Line Manager in the first instance to decide the next steps and how to deal with it.

- Make copies of the relevant offensive comments if possible (for example, by taking screen shots).

- If the posts are discriminatory or could constitute criminal behaviour, discuss with your Line Manager in the first instance and Corporate Communications/People Services/Legal for consideration as to whether to refer to the Police.

Bullying and Harassment from Councillors

Abusive comments made by councillors on social media, carried out in an official capacity, could constitute a breach of the member Code of Conduct as this requires councillors to, 'treat others with respect'.

The employee's Manager should refer the matter to the Monitoring Officer for advice. The advice will be fed back and if necessary the complaints process will be explained to the employee and could be submitted by the Line Manager or Director.

Bullying and Harassment from Members of the Public

Complaining Posts

Posts may be made by members of the public, complaining that a certain course of action has been taken, or not taken by an officer, the Council/school. Complaints direct to Council's social media sites or employees' work accounts should in the first instance try to be dealt with through the channel the complainant has contacted

the Council on, ie social media. This can be done by responding publicly to the post if the response will be of benefit to the wider public or through direct messaging if it is felt that the matter should be dealt with more discreetly. The Manager may consider that the issue can only be resolved by speaking with the complainant to discuss the comments. If such a discussion takes place, the Manager should make it clear that the way in which to submit an official complaint is to use the formal complaints system and make it clear that the postings need to be removed from the social media site.

Abusive Posts

If comments/complaints target an individual employee specifically, eg abusing the employee, questioning an employee's integrity or making allegations that an employee has made a decision or dealt with a matter in a way that shows an ulterior motive, such as a vendetta against someone, friendships or the payment of monies, Managers should consider:

(a) If the person can be identified who has made the abusive posts, whether it would be appropriate for a letter from the Manager or Director to be sent to the person making the comments, making it clear that the Council considers that such posts are unacceptable and the Council will support their employee. Such a response should be considered on a case by case basis.

(b) Whether such a response would simply be 'feeding' the person making the comments, that responding will simply encourage further posts.

(c) Whether the best approach is to simply ignore such posts. Where the abuse is channelled through a Council Facebook account or personal/work account, when appropriate this can be done by hiding the comments/complaints from public view so they can only be seen by the person who wrote the post and their friends. Or consider blocking the individual altogether from the social media channel they are using.

In some cases, the person may simply have been venting their feelings and by choosing not to respond no further comments are made. Engaging with the person may escalate the situation. In many cases the general public will respond to negative comments therefore diffusing the situation without the Council having to become involved.

Employees should not post unguarded or hasty comments on social media in response to any abuse. Such comments, if regarded as offensive, could lead to complaints being made against them.

Abuse - Criminal

In order for comments on social media to be considered criminal acts they must contain threats to carry out criminal acts or the posts must constitute a course of conduct that amounts to harassment.

Posts which threaten to kill, attack or otherwise harm an individual, or threats to destroy or damage property, should be reported to the Police.

A series of posts on social media can constitute criminal behaviour if the comments made potentially amount to harassment of another, and the person making the posts knows or ought to know amounts to harassment of another. In determining whether the person whose course of conduct is in question ought to know that it amounts to harassment of another, the test is whether a reasonable person in possession of the same information would think the course of conduct amounted to harassment.

If an employee considers that a series of posts about them amount to harassment

they should follow the advice set in in the General Principles listed above.

12. References

Social Media Guidance for Civil Servants
Cabinet Office.

APPENDIX 1

Social Media Guidance Q and A

1. What is social media?

'Social media' is the term commonly given to websites and online tools which allow users to generate their own media and interact with each other in some way.

2. Can I access social media at work?

Yes, you are permitted to access social media sites for example Facebook, Twitter and YouTube from a Council computer for work use during working hours. If a login is required you will need to set up a work social media account. Please refer to the Social Media Guidance for more details. For personal use, social media should only be accessed during your own time, please see the Social Media Guidance for more details. Contact the Corporate Communications team at social.media@eastriding.gov.uk for advice.

3. How do I set up a work social media account?

If employees require a work account, permission must be sought and supported by the employee's Line Manager. Managers must agree in advance the scope, context and timings of social media work accounts. When applying employees need to state which platforms they require work accounts for, clearly detailing the reason why the work account is required. Access to the social media work account request e-form is accessed via the social media section of the intranet, at http://insight.eastriding.gov.uk/socialmedia.

The eform will be submitted to the Corporate Communications team for consideration. Work accounts if approved will be set up by the Corporate Communications team. Staff must not set up their own accounts. It is important for audit purposes that the Council maintains a list of staff who have work accounts.

4. Friends with customers/members?

It is not advisable to become friends with customer/clients on personal social networking sites. The Code of Conduct for Employees also makes it clear that close personal familiarity between elected members and officers is to be avoided. On work social media accounts the employee must maintain a professional relationship at all times with the individual or organisation.

5. Do you want to post to the corporate social media accounts?

The Corporate Communications team are responsible for the corporate social media accounts. The team use a range of platforms and will help you to consider which is best for your needs. You should firstly consider how your customers want to be communicated with and how social media can be used as part of a mix of communications techniques. Social media is a cost-effective way of reaching your customers if they are responsive to this method. Consider how social media can promote your service, raise awareness of important information or encourage your customers to self-serve using the web and other digital channels. You will need to ensure you have the relevant website content and electronic forms in place for this to be achieved. Contact the team at social.media@eastriding.gov.uk for advice.

6. Can I post onto social media in my works capacity?

You are able to post on social media for work purposes if you have a work social media account and it has been agreed with your Line Manager that the purpose of you having that account is to post in your professional capacity. Personal social media accounts should not be used for work purposes, with the exception of professional networking sites such as LinkedIn. Permission has to be obtained in advance from your Line Manager. You must always identify yourself as speaking on behalf of the Council when posting in a works capacity to comply with RIPA Policy and Procedures as detailed in the Social Media Guidance.

Before posting on your work account, please be aware that you are representing the Council and you must ensure the information you are communicating is correct. Once you post on social media you are then open to comments from the general public, any subsequent correspondence should be dealt with in a professional manner as you would any other form of communication.

7. Using social media for work?

You should participate in the same way as you would with other media or public forums such as giving presentations:

- Be aware; understand what permissions and for what purpose you are allowed to access social media. Do not log in to social media using a personal account for work purposes, you cannot control the content of others and may contravene the Council's policies.
- Be professional; remember that you are an ambassador for the Council. Anything you publish will reflect directly on the Council as a whole.
- Be responsible; be honest at all times and when you gain insight share it with others where appropriate.
- Be credible; be accurate, fair and thorough and make sure you are doing the right thing.
- Be safe; never give out personal details like home address and phone numbers, or any financial details.

8. Using social media for personal use?

The Council expects the highest standards of behaviour from its employees and staff should apply the same standards of conduct online as they are expected to apply offline. If you use social media for personal use in your own time, be careful that any comments you make are carefully considered as any inappropriate comments could impact on the Council's reputation. Misuse of social media is taken very seriously. Any misuse can result in action being taken under the Council's Disciplinary Policy which can result in dismissal.

Employees should be aware that nothing they post on social media is ever truly private, information published online can be accessed around the world within seconds and will be publicly available for all to see.

9. Cyberbullying

Bullying and harassment using social media platforms is increasing. If you become the subject of bullying and harassment you should report it to your Manager, as outlined in section 11 of the Guidance on the use of Social Media. Dependent on the nature and source of the harassment it may be possible to take further action.

Any queries email social.media@eastriding.gov.uk.