E-SAFETY POLICY

Policy adopted by the Governing Body of The Wordsley School	
Date adopted by the Governing Body	**26th February 2025**
Signed by the Chair of Governors	**N Hubbard**

Online Safety in Schools

School, College or Other Provider:	*The Wordsley School*	
Author/Owner:	Andrew Fisher	Assistant Headteacher
Accountable Headteacher:	*Ashley Weatherhogg*	*Head Teacher*
Approved by (Board of Directors/Governing Body/Governors Sub Committee):	*Name:*	*Signature:*
Date of Approval:		
Monitoring and Revision due:	*The online safety policy will be reviewed annually. It will also be reviewed to align with national, regional and local legislative or statutory changes.* *The next anticipated review date will be: February 2026*	

Policy Overview:
The purpose of this policy is to safeguard and protect all members of The Wordsley School 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 The Wordsley School. This includes staff, students, volunteers, parents/guardians/carers, visitors and community users who have access to and are users of The Wordsley School digital technology systems, both internally and externally.

References:
Department for Education (DfE) (2024) Keeping Children Safe in Education: statutory guidance for schools and colleges. London: DfE. 2 September 2024 Department for Education (DfE) (2019b) Teaching online safety in school: guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. London: DfE. Department for Education (DfE) (2018) Working together to safeguard children. London: DfE Department for Education (2014) Cyberbullying: Advice for headteachers and school staff. London: DfE. Children Act 1989 Children Act 2004

Communications Act 2003

Computer Misuse Act 1990

Criminal Justice and Courts Act 2015

Data Protection Act 1998

Data Protection Act 2018

Education Act 2011

Education and Inspections Act 2006

Freedom of Information Act 2000

Malicious Communications Act 1988

Serious Crime Act 2015

Voyeurism (Offences) Act 2019

This policy links with other policies and practices

- Anti-bullying
- Acceptable Use Policies (AUP)
- Behaviour and discipline policy
- Child protection policy
- Complaints policy
- Confidentiality and data protection policy
- Curriculum policies
- Use of images policy

Disclaimer

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. If errors are brought to our attention, we will correct them as soon as is practicable.

CONTENTS

1. 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 The Wordsley School. This includes staff, students, governors, volunteers, parents/guardians/carers, visitors and community users who have access to and are users of the The Wordsley School digital technology systems, both internally and externally within the home and community setting.

2. Online Safety School Statement

The Wordsley 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.

The Wordsley School believes that the internet and associated devices are an integral part of everyday life

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

3. 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 (2024), 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, 2020).

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 the associated statutory legislation and guidance as stipulated on page 1-2 of this policy.

4. Roles and Responsibilities

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

4.1 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.

4.2 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.

4.3 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/carers 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.

4.4 Children and Young People

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

- Know who the DSL/Deputy 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 UK Council for Child Internet Safety (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

4.5 Parents/ Carers

Parents/ Carers need to understand the risks that children face online to protect them from online dangers. parents/carers 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.

5. 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 rely 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.

5.1 Learners

The Wordsley 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.

The Wordsley 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.

5.2 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.

The Wordsley 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.

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

5.3 Staff

The Wordsley School will:

- Ensure provision of robust policies and practices as part of induction and ongoing training provision.
- Sign and adhere to Section 14 of this policy
- 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.

5.4 parents/guardians and carers

The Wordsley School will:

- Recognise and cultivate the essential role parents/guardians 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).

6. 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

6.1 Evaluate: How to evaluate what they see online

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

The Wordsley School will help students 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?

6.2 Recognise: How to recognise techniques used for persuasion

This will enable students 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.

The Wordsley School will help students 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.

6.3 Online Behaviour

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

The Wordsley School will help students 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.

6.4 Identify: How to identity online risks

This will enable students 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 students assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

The Wordsley School will help students 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?

6.5 How and when to seek support

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

The Wordsley School will help students 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.

7. 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 The Wordsley School 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 The Wordsley School local process.
- Always adhere to local safeguarding procedures and report to the DSL and Headteacher.

8. 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 (with the exception of the headteacher) to inform their line manager iif 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 becomes subject to adult protection matters. The line manager must report this to the DSL and Head Teacher.

9. Monitoring and Compliance

This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

to establish the existence of facts;

to ascertain compliance with applicable regulatory or self-regulatory practices or procedures;
to ascertain or demonstrate effective system operation technically and by users;
for national security/crime prevention or detection; for confidential counselling/support services;
for investigating or detecting unauthorised use of the system;

for monitoring communications for the purpose of determining whether they are communications relevant to the business.

Research Machines (RM) has a contractual obligation to monitor the use of the internet, email and school network services provided as part of DGfL (Dudley Grid for Learning), in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the Wordsley School reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from Governors, employees or any other authorised users the facility to send and receive electronic communications.

If the email is personal, it is good practice to use the word ‘personal’ in the subject header and the footer text should indicate if it is a personal email. The school does not accept responsibility for any agreement the user may be entering into.

Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School’s business purposes which include the following:

providing evidence of business transactions;

making sure the School’s business procedures are adhered to; training and monitoring standards of service;
preventing or detecting unauthorised use of the computer systems or criminal activities;

maintaining the effective operation of communication system.

The school currently uses a variety of network packages to:

manage all users and set permissions for access; provide school filtering of the internet on site; provide school network security;
monitor all activity on the school network;

proactive safeguarding monitoring (E-safe forensics)

10. Financial Risk Assessment

There are no financial risks associated with this policy

11. Consultation / Approval Process

This policy has been developed in conjunction with the online safety working group and approved by the Joint Negotiating and Consultative Committee

12. Dissemination and Communication Process

The policy will be placed in the Whole School Policy Folder, on the school website and will be publicised through an induction and training update and notified to the Governors Board.

13. Development of the Policy

This policy will be reviewed annually, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

14. Specific Staff Policy

(i) INTRODUCTION

The internet and email play an essential role in the conduct of our business in education. The systems within school are made available to Students, Teaching Staff, Support Staff, Governors and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been significant investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of email, school network and the internet.

We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this policy.

For your safety and safeguarding, we are able to monitor all network traffic, web pages visited, email sent and received, this helps us monitor inappropriate use, such as bullying and any inappropriate or unlawful behaviour.

This policy applies to you as a Governor, as an Employee or individual granted with access to the school's network, whatever your position, whether you are a Head teacher, Teacher,

Support Staff, permanent, temporary or otherwise and any other authorised users. Any inappropriate use of the School's internet, email and computer systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head teacher.

(ii) GENERAL PRINCIPLES and LEGAL ISSUES

All information relating to our pupils, parents/guardians and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically and understand processing and storage of data must be compliant with the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018.

Care must be taken when using email as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

We trust you to use the internet sensibly. Please be aware at all times that when using the internet, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.

The main advantage of the internet and email is that they provide routes to access and disseminate information. However, the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example,

sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing, (Communications Act 2003, Protection from Harassment Act 1997, Racial and Religious Hatred Act 2006). Internet and email access is intended to be used for school business or professional development, any personal use should only be by prior agreement with the Head teacher and is subject to the same terms and conditions.

As an Employee, Governor or any other authorised user, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data should be in accordance with the requirements and principles of the GDPR (General Data Protection Regulations) 2016 and the Data Protection Act 2018. Schools are defined in law as separate legal entities for the purposes of complying with the GDPR and Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights (Copyright, Design and Patents Act 1988).

(iii) USE OF THE SCHOOL NETWORK

New staff (and all other new authorised users) either temporary or permanent will receive an e-safety induction with the IT Manager and sign the school e-safety policy before new users are issued with a unique network id and password to access the school network.

Access to the management information system will require separate authentication with a unique password and only given to staff with appropriate permissions by the Senior Administrator.

Concurrent log-ons are not allowed on the school network this means a user can only log-on to one computer at a time.

Passwords should be changed on a regular basis, the school network forces users to change their password every 90 days, using only strong passwords with a minimum of 8 characters. These passwords cannot be reused.

Staff and all other authorised users must not share their passwords or their user area with any other member of staff, pupil or guest.

Workstations should be locked if unattended for any duration to avoid loss of work or potential data protection breach (workstations automatically lock after 5 minutes when inactive).

Projection should be blanked when navigating your user area or using the school Management Information System; SIMS, to avoid any potential data protection breach.

Anyone wishing to use the School Wi-Fi/network to access the internet or network on their own personal laptop or any other mobile device must sign the School Personal Device Agreement.

When accessing any of the school systems from home, at work or any other location, always be aware of the schools Data Protection Policy, GDPR (General Data Protection Regulations) 2016 and the Data Protection Act 2018 by keeping digital information or documents away from unauthorised persons. It is also expected and good practice to do the following:

keep your laptop/computer or other device updated with the latest operating system patches/updates, antivirus/malware/spyware software and run these regularly;

keep your logon credentials secure and private; do not allow access to unauthorised persons; change your password regularly with a strong password. If using a mobile device, the password must have a minimum of 6 digits.

Do not store any sensitive information/data locally on the device;

Do not leave your device unattended when logged in to a remote session, make sure you have logged out properly.

(iv) USE OF INTERNET, Google for Education VLE and SHAREPOINT

When using the internet, always read and comply with the terms and conditions governing the sites use.

Do not download any images, text or material which is copyright protected without the appropriate authorisation (Copyright, Design and Patents Act 1988).

Do not download any images, text or material which is inappropriate or likely to cause offence.

If you want to download any software on the school network, first seek permission from the Head teacher and/or IT Manager /RM. They should check that the source is safe and appropriately licensed.

Access to YouTube for the purpose of teaching and learning is now allowed for Staff through Dudley MBC's default filtering policy. However, it is only authorised for use in safe search mode and it is your responsibility to check that all content is appropriate for the education environment.

If you are involved in creating, amending or deleting our web pages or content on our web sites, Google for Education VLE or SharePoint, such actions should be consistent with your responsibilities and be in the best interests of the School.

You are expressly prohibited from:

introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software or any software which could compromise network security;

seeking to gain access to restricted areas of the network;

knowingly seeking to access data which you are not authorised to view;

introducing any form of computer viruses or software/programs which could compromise network security and

carrying out any hacking or any unauthorised activities.

For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

unauthorised access to computer material i.e. hacking;

unauthorised modification of computer material; and

unauthorised access with intent to commit/facilitate the commission of further offences.

(v) USE OF ELECTRONIC MAIL

You should agree with recipients that the use of email is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted email is not secure.

Emails to Dudley MBC including Dudley Schools are secure however do not send any sensitive personal data via email unless you are using a secure site or portal.

It is good practice that sensitive documents or attachments should always be encrypted before sending. It is also good practice to indicate that the email is 'Confidential' in the subject line.

Copies of emails with any attachments sent to or received from parents/guardians should be saved in a suitable secure directory on a secure system.

Do not impersonate any other person when using email or amend any messages received. Do not disclose or show emails to any unauthorised persons.

It is good practice to re-read emails before sending them as external emails cannot be retrieved once they have been sent.

It is good practice to change your email password on a regular basis; this should be a strong or secure password using a minimum of 8 alphanumeric characters including numbers, special characters, upper and lower case letters.

Email should be used for school and educational purposes only please refer to general principles and legal issues for acceptable use of email.

(vi) DATA PROTECTION (GDPR 2016 and Data Protection Act 2018)

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must:

familiarise yourself with the principles of the General Data Protection Regulation 2016 and Data Protection Act 2018 and work in accordance with these guidelines;

familiarise yourself with the School Data Protection Policy, Freedom of Information Policy, Information Security Policy and procedures;

undertake the online Data Protection, Freedom of Information, Information Security training modules;

keep the data private and confidential at all times by not accessing the school network or management information system or data in locations where information can be read or accessed by unauthorised persons;

keep information and data private when working from home, you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head teacher or line manager;

keep data secure at all times by only accessing and storing it on an authorised secure system and if using a mobile device do not store information on any device which is not encrypted;

always use secure storage of documents and equipment containing sensitive data (documents or equipment should never be left in the car or any other place where unauthorised persons can read or gain access to data);

sensitive data should only be accessed using the secure school network systems and should never be stored locally on mobile devices and computers which are not encrypted;

not make personal or other inappropriate remarks about staff, pupils, parents/guardians or colleagues on manual files, computer records, email or social media. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

The School views any breach of the GDPR (General Data Protection Regulations) 2016 and Data Protection Act 2018 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures. If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.