Meole Brace School

E-Safety Policy 2019/20

This Policy has been agreed by the following professional associations and Trade Unions representing Teachers, Headteachers and Support Staff:

- National Education Union
- National Association of Schoolmasters Union of Women Teachers
- National Association of Headteachers
- Association of School and College Leaders
- Unison
- GMB

This policy has been adopted by the governing body

on

and will be ordinarily reviewed every year

CONTENTS

E-Safety Policy

1. Introduction

This policy has been written by colleagues from Human Resources (HR), the Education Improvement Service (EIS) and Shropshire Safeguarding Children Board (SSCB). It has been created to support school leaders in addressing whole-school issues in the use and application of new and emerging technologies across the school community. Shared ownership of this policy ensures both consistency of approach, and efficiency in relation to its ongoing review, update and/or revision to content.

E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media (e.g. text messages, email, gaming devices etc.).

E-safety is not just about technology, it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities; online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they shouldn't, or be treated by others inappropriately.

E-safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside, is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Sex and Relationship Education (SRE) and include how students should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc)

General advice and resources for schools on internet safety are available at:
https://www.saferinternet.org.uk/

In association with the appropriate Acceptable Use Policy Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Child Protection/ Safeguarding, Behaviour and Anti-Bullying policies.

In England, schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. Since 2015 there have been additional duties under the Counter Terrorism and Security Act 2015, known as the 'Prevent duty', which require schools to ensure that children are safe from terrorist and extremist material on the internet, to prevent people from being drawn into terrorism.

Ofsted judges as 'outstanding', schools where '*students have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites*'.
(*Source: Ofsted School Inspection Handbook - October 2017)*

This policy will be reviewed annually and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or the level and/or nature of incidents reported.

2. Scope

This policy applies to all members of the school community, including staff, governors, students, volunteers, parents, carers, visitors {and community users}. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-

bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school.

The school will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices. In the case of both acts, action will be taken in line with the school's published Disciplinary Procedure and/or Behaviour Policy.

The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date and reflect changes or amendments such as a member of staff who has left the school or a student whose access has been withdrawn.

3. The Prevent Duty

As organisations seek to influence young people through the use of social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are required to identify risks within a given local context and identify children who may be at risk of radicalisation, and know what to do to support them.

The Prevent duty requires school monitoring and filtering systems to be fit for purpose. The school has a filtering system in place and its effectiveness is monitored by Chris Williams (Network Manager)

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

All staff should be aware of the following:

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel

4. Terrorism Act 2000 and the disclosure of information duty where it is believed or suspected that another person has committed an offence.

Practical advice and information for teachers, parents and school leaders on protecting children from extremism and radicalisation is available at:

https://www.educateagainsthate.com/

The Department for Education has dedicated a telephone helpline (020 7340 7264) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by email to:

counter.extremism@education.gsi.gov.uk

Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed.

4. Governing Legislation

It is important to note that in general terms an action that is illegal if committed offline, is also illegal if committed online.

Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers 2000
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1998

The Education and Inspections Act 2006
The Education and Inspections Act 2011
The Protection of Freedoms Act 2012
The Schools Information Regulations 2012
Serious Crime Act 2015
Terrorism Act 2000

Further explanatory detail about governing legislation can be found in Appendix G.

5. Roles & Responsibilities

{nb. if the *school / academy* has a managed ICT service provided by an outside contractor, it is the responsibility of the *school / academy* to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff. The managed service provider should be fully aware of the *school/academy* E-Safety Policy and procedures.}

E-safety is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

Head/Principal	Mrs A Doust
E-safety Coordinator /DSO/CPO/HEAD/LEAD TEACHER of ICT	Mr S. Iddon
Head of ICT/Lead teacher for ICT	Ms J Hughes
Network Manager/Technician	Mr C Williams

A full description of the responsibilities associated with these roles may be found in Appendix F.

6. Definitions: Devices & Technology

Device(s)	Examples include but are not limited to: • Personal computers • Laptops • Tablets • 'Smart'/Mobile phones • 'Smart' watches • Cameras • USB sticks/flash drives
Technology(ies)	Examples include but are not limited to: • Internet search engines • Websites • Social media platforms, e.g. Facebook, Twitter, Instagram, Snapchat, WhatsApp, YouTube • Real time communications e.g. texts, chat rooms, email, instant messaging, Skype, FaceTime, video chat • On-line gaming, e.g. Xbox, PlayStation

7. School Staff, Governors and Volunteers

Acceptable Use Policy Agreements

Before being granted access to school devices and technologies, all members of the school community are required to read and sign an Acceptable Use Policy Agreement (AUP), appropriate to their role and status in school.

The AUP for staff has been created by HR. The AUP for staff may be used and/or adapted for any user, to include governors, volunteers and community users.

Acceptable Use Policy (AUP) for Staff

The AUP for staff can be found in Appendix A

All staff must read and sign the 'Acceptable Use Policy Agreement for Staff' (AUP) before using any school IT resource. Differing versions of this agreement may be used to match the personal and professional roles of staff members.

A copy of the staff AUP will be issued to all new members of staff during Induction. The school will also issue the AUP to staff, periodically, in response to the nature and/or volume of reported incidents, changes in legislation and emerging trends in online behaviour.

Access to online services and school devices will not be approved until new staff have signed and returned the AUP. Access may be suspended or restricted for serving staff who do not return an AUP issued on a periodic basis.

Staff are required to accept the general principles of acceptable use of school devices and technologies each time they log in to a school device.

E-safety and the AUP are included in the statutory induction for all new staff and forms part of the contract of employment.

Acceptable Use of Devices and Technologies: Staff

Any device provided by the school, to or for staff or students, is primarily intended to support the teaching and learning of students. Discretion and the highest professional standards of conduct are expected of staff using school devices for personal use.

Where remote access to the school network via a personal device is approved by the Headteacher, staff confirm their acceptance of the terms set out in the Acceptable Use Policy in relation to that device. Staff should seek clarification of any terms and conditions they do not understand.

Staff breaches of the AUP

Where a staff member is found to be in breach of the Staff AUP, the matter will be dealt with in accordance with appropriate school policies such as the Disciplinary procedure, and /or with reference to external agency guidance.

8. Students

Acceptable Use Policy (AUP) for Students

The AUP for students can be found in Appendix B, C & D.

A copy of the student AUP is sent to parents with a covering letter/reply slip, at the start of the academic year, and to new students when they enrol. Students will not be given online access or allowed to use school devices before the AUP has been signed and returned to the school office.

It is also available to download on the school website and as a printed version in the student planner.

The student AUPs have been created by the Education Improvement Service. They have been written to be relevant to and appropriate for different age groups, and can be found in Appendices B C and D.

Acceptable Use of Devices and Technologies: Students

Students are required to accept the general principles of acceptable use of school devices and technologies each time they log in to a school device or the school network.

Student breaches of the AUP

Where a student is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

Examples of scenarios which may give rise to an E-safety concern are set out in Appendix I.

Remedial action and sanctions are at the discretion of school management. Outline guidance for teaching and leadership staff is set out in Appendix J.

9. Using non-School Equipment – 'Bring Your Own Device/Bring Your Own Technology' (BYOD/BYOT)

Under some circumstances, staff, governors and students are able to use their own devices in school and connect to the school network. This is normally referred to as 'Bring Your Own Device'/'Bring Your Own Technology' (BYOD/BYOT).

Regardless of the ownership of the device, the rules and expectations of online behaviour are as set out in the relevant AUP.

10. Security and passwords

Passwords should be changed regularly and must not be shared. The school system will inform users when the password is to be changed. Staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended.

NB. The picture 'mute' or picture 'freeze' option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'.

All users should be aware that the ICT system is filtered and monitored.

11. Data storage

Only encrypted USB pens are to be used in school. For further clarification, please contact Chris Williams (E-safety Coordinator/Network Manager) All devices that contain student information must be encrypted. Staff devices can be encrypted.

12. Mobile phones, cameras and other devices

The school's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP.

Student devices such as mobile phones, should be switched to silent whilst on the school premises and kept out of sight. Students found to be in breach of this requirement will have their device confiscated and sent to the school office in a sealed envelope marked with the student's name and class/form.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated and the matter dealt with in line with normal school procedure and/or the Behaviour policy.

All staff are required to adhere to the AUP which sets out the expected use of mobile phones whilst on duty.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection Act.

13. Social Media and Networking

The expectations around the use of social media are set out in the relevant AUP.

14. Cyber bullying

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school must have measures in place to prevent all forms of bullying. These measures

should be part of the school's behaviour policy which must be communicated to all pupils, school staff, governors and parents.

Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

Cyberbullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Please refer to Appendix L for further guidance and support in dealing with instances of cyberbullying against staff and/or students.

15. Staff Reporting of E-safety Incidents and Concerns

The school takes the reports of incidents and concerns extremely seriously. Any subsequent action or remedy to be taken following the investigation of an incident or concern, will depend on its nature, situational and circumstantial factors.

All incidents that come to the attention of school staff should be notified to the E-safety Coordinator – Simon Iddon via the school reporting mechanism set out in Appendix K, or, where applicable, via the Whistleblowing Policy.

Any incident that raises child protection or wider safeguarding questions must also be communicated to the Designated Safeguarding Lead(s) immediately.

Incidents that are of a concern under the Prevent duty should be referred to the E-safety Coordinator and/or designated Safeguarding Lead, immediately.

Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT or CL, immediately.

Examples of potential E-safety concerns may be found at Appendix I.

16. Staff training and updates

All staff have E-safety training included as part of their safeguarding induction to the school and receive regular training in safeguarding students. E-safety is included as part of this.

E-safety incidents and concerns are a standing item at staff briefings.

17. Communicating the E-safety Policy

Staff and the E-safety policy

- All staff will be given a copy of the E-safety Policy during statutory induction and its importance explained.
- An Acceptable Use Policy Agreement is signed before access to school devices and systems is approved and the agreement forms part of the contract of employment.
- Staff are made aware that internet traffic can be monitored and traced to the individual user, including on personal devices where network access has been granted. Because of this, discretion and professional conduct are essential at all times.

Introducing the E-safety policy to students

- The E-safety Policy/Acceptable Use Policy Agreement is/are posted in all classrooms, as appropriate, and its content referred to on a regular basis. The aim is to make the policy familiar and accessible to all students at all times.
- Students are made aware that network and Internet use is monitored.

Home-School Communication of E-safety information

- The school website provides information on E-safety and how the school can help to support and guide their child
- E-safety advice is included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- The school holds E-safety events to brief parents and carers about E-safety developments and policies.

18. Shropshire Safeguarding Contact details:

Local Authority Designated Officer (LADO) lado@shropshire.gov.uk
Emergency Duty Team 0345 678 9040
01743 249544 (Out of hours only)

19. Monitor & review

This policy will be monitored continuously. It will be reviewed annually, and/or more frequently in line with new developments in the use of the technologies, new threats to online safety or level and/or nature of incidents reported.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Meole Brace School must ensure that:

- **it has a Data Protection Policy. (see appendix for template policy)**
- **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).**
- **it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.**
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it**
- **the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded**
- **it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
- **it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
- **procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).**
- **data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)**

- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- **it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.**
- **it understands how to share data lawfully and safely with other relevant data controllers.**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

When personal data is stored on any mobile device or removable media the:

- **data must be encrypted and password protected.**
- **device must be password protected.**
- **device must be protected by up to date virus and malware checking software**
- **data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.**

Staff must ensure that they:

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school**
- **where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.**
- **will not transfer any school/academy personal data to personal devices except as in line with school policy**
- **access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data**

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school/academy* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school/academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. NOS online training.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school/academy social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school/academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school/academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school/academy permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's/academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Appendix A - AUP for Staff {Governors & Volunteers}

I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.

I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

- I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.
- I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.

- {I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.}
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should keep passwords safe and not share them with anyone.
- I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.
- I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.
- I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy).
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving devices or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will log out of a device when I have finished using it.

Electronic communications and use of social media:

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.
- I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident.
- I will not, under any circumstances, make reference to any staff member, student, parent or school activity/event via personal social media or other communication technologies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.
- I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.
- I will not use the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material, online or in print.
- I will not post any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies

- When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.
- I will keep mobile devices switched off and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.
- I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.

- I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.
- I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
- I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.
- I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above, and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.

I understand that in the event of any query or concern about this Agreement, I should contact Simon Iddon.

Staff / Volunteer Name:	
Signed:	
Date:	

Appendix B - AUP for learners in KS3 and above

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- respect the school network security
- set strong passwords which I will not share other than with my parents.
- only use, move and share personal data securely
- not use my own mobile phone, or any other device, in school, unless I am given permission
- only visit sites which are appropriate
- always follow the terms and conditions when using a website
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- discuss and agree my use of a social networking site with a responsible adult before joining
- not access social networking sites whilst at school
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online at school via the school network may be monitored by the school.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I am aware of the CEOP Report button and know when to use it.

I agree that I will not:

- act in a way that might breach the school Behaviour policy
- forward chain letters
- breach copyright law
- do anything which exposes others to harm or danger
- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts

I accept that my use of both school and personal devices may be monitored and reported on.

Signed _____ ***Date*** _____

Home-school E-safety; ICT, Mobile Phones, Personal Photographs and Social Media

Student Name	
Student's class teacher/form name	
Parent/Carer/Guardian's name	

Use of School ICT Equipment and Internet Access

As the parent or legal guardian of the above-named student, I give permission for my child to access the Internet, the school email and other ICT facilities, whilst at school. I understand that my child has signed an Acceptable Use Policy (AUP) confirming their understanding and acceptance of the proper use of school and personal ICT equipment. I also understand that my child may be informed, should the rules change or be updated, during the year.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent them from accessing inappropriate materials. These steps include the school using a filtered internet service, providing secure access to email, employing appropriate teaching practice and teaching e-safety skills to students, across the curriculum.

I understand that the school can monitor my child's computer files and the Internet sites they visit. I also understand that the school may contact me if there are concerns about my child's online behaviour or safety. I will support the school by promoting safe use of the internet and digital technology at home, and will inform the school if I have any concerns about my child's e-safety.

Mobile Phones and other Personal Devices

I understand that unless my child is given permission by a teacher, their mobile phone and any other personal device should be switched off and kept out of sight during the school day. This includes during off-site activities; if a device is used without permission it will be confiscated until the end of the school day.

Personal Photographs and Social Media

I am aware that the school permits parents/carers to take photographs and videos of their own children at school events but requests that where the photos/videos contain images of other children, these are not shared on any social networking site such as Facebook or Instagram. I will support the school's approach to e-Safety and will not post, upload or add any text, image or video that could upset, offend or threaten the safety of any member of the school community

Signature of Parent/Carer/Guardian:

Date:

Appendix C

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. *Students/Pupils* and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school/academy is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school/academy website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name:..... Student/Pupil Name:.....

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No

• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
Insert statements here that explicitly detail where images are published by the school/academy	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....
Date: .....

Appendix D

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils/students.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses **insert cloud service provider name** for *pupils/students* and staff. This permission form describes the tools and pupil/student responsibilities for using these services.

The following services are available to each *pupil/student* as part of the school's online presence in **insert cloud service provider name**

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

As the school/academy is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared
Where this form will be stored.	Who the data will be shared with
How long this form will be stored for.	Who will have access to the data.
How this form will be destroyed.	Where the data will be stored.
	How long the data will be stored for.
	How the data will be destroyed.
	How a request for deletion of the data can be made.

Do you consent to your child to having access to this service? Yes/No

Student/Pupil Name: ..... Parent/Carers Name: .....
Signed: ..... Date: .....

Appendix E

Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school/academy is collecting special category personal data and **delete as appropriate** sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared
Where this form will be stored.	Who the data will be shared with
How long this form will be stored for.	Who will have access to the data.
How this form will be destroyed.	Where the data will be stored.
	How long the data will be stored for.
	How the data will be destroyed.
	How consent to process the biometric data can be withdrawn.

Parent/Carers Name: .....

Student/Pupil Name: .....

As the parent/carer of the above student/pupil, I agree to the school using biometric recognition systems, as described above.	Yes/No
I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school.	Yes/No

Signed: .....

Further guidance

- Each parent of the child should be notified by the school/academy that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school/academy to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' consent.

- Schools and colleges must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the student/pupil attends the school, but new permission is required if there are changes to the biometric systems in use.

Appendix F: E-safety Roles & Responsibilities: List of duties

Head/Principal	• Has overall responsibility for E-safety provision. • Has overall responsibility for data and data security • Ensures that the school uses an appropriate filtered Internet Service • Ensures that staff receive appropriate training to enable them to carry out their E-safety roles • Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Receives regular monitoring reports from the E-safety Coordinator/Officer. • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews (e.g. Network Manager). • Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach.
E-safety Coordinator /Designated Safeguarding Lead/CPO/HEAD/LEAD TEACHER of ICT	• Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies and supporting documents. • Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Promotes an awareness of and commitment to E-safety throughout the school community. • Ensures that E-safety is embedded across the curriculum. • Is the main point of contact for students, staff, volunteers and parents who have E-safety concerns. • Ensures that staff and students are regularly updated on E-safety issues and legislation, and are aware of the

	potential for serious child protection issues that arise from (for example): - sharing of personal data - access to illegal/inappropriate materials - inappropriate on-line contact with adults/strangers - cyber-bullying • Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • Ensures that an E-safety incident log is kept up to date. • Liaises with school IT technical staff where necessary and/or appropriate. • Facilitates training and provides advice and guidance to all staff. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering.

Head of ICT/Lead teacher for ICT	• Oversees the delivery of the E-safety element of the Computing curriculum. • Communicates regularly with the E-safety coordinator.
Network Manager/Technician	• Oversees the security of the school ICT system. • Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software). • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Ensures that the school's policy on web-filtering is applied and updated on a regular basis. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that users may only access the school networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Reports any E-safety incidents or concerns, to the E-safety co-ordinator. • Keeps up to date with the school's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school systems.

ALL Staff	• Read, understand and help promote the school's E-safety policies and guidance. • Are aware of E-safety issues relating to the use of any digital technology, monitor their use, and implement school policies with regard to devices. • Report any suspected misuse or problem to the E-safety coordinator. • Maintain an awareness of current E-safety issues and guidance, e. g. through training and CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with students are on a professional level and through school-based systems ONLY. • Ensure that no communication with students, parents or carers is entered into through personal devices or social media. • Ensure that all data about students and families is handled and stored in line with the principles outlined in the Staff AUP.
Teaching Staff	• Embed E-safety issues in all aspects of the curriculum and other school activities. • Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities, where relevant). • Ensure that students are fully aware of how to research safely online and of potential legal issues relating to electronic content such as copyright laws.
Students / Students:	• Are responsible for using the school digital technology systems in accordance with the Student AUP Agreement. • Have a good understanding of research skills, the need to avoid plagiarism and to uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. • Understand policies on the use of mobile devices and digital cameras, the taking and use of images and cyber-bullying. • Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions, in and out of school, if related to their membership of the school.

Parents / Carers	Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events. • access to parents' sections of the website/ Learning Platform and on-line student/student records. • their children's personal devices in the school.
External groups	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Appendix G: Legislation - Overview of relevant legislation governing E-safety

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

It is recommended that HR and/or legal advice is sought in the event of an E-safety incident or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 1998

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

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

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

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence, liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority, intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as 'fair dealing', which means, under certain circumstances, permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear, on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet), it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification, or that of others. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any person having sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view to releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence

- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced the new offence of sexual communication with a child. Also created new offences and orders around gang crime (including Child Sexual Exploitation (CSE)).

Appendix I: Examples of potential E-safety concerns (Students)

The following are provided by way of guidance and are in no way limiting or exhaustive. You should seek advice from the E-safety coordinator if you are unsure about what might constitute a concern.

Inappropriate material accessed on school computers

Due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

Students are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to the E-safety Co-ordinator who will log the problem and liaise with the Network Manager to make any necessary adjustment to filter settings.

Abusive messages on school computers

Students who receive abusive messages over school systems will be supported, and advised not to delete messages. The E-safety Co-ordinator will be informed and a formal process of investigation initiated.

Parent/Carer/Guardian reports of cyber bullying

Parents, carers and guardians may become aware that their child is concerned or upset by bullying, originating in the school but continuing via electronic means. Parents and carers should know that the school encourages them and/or students to approach them for help, either via a staff member or directly to the Head. Such incidents will be investigated and dealt with in accordance with the school/academy Behaviour/Bullying policy.

Student disclosure of concerns or abuse

All staff receive Safeguarding and E-safety training as part of their induction, and thereafter on a regular basis. Where a student discloses a concern to a member of school staff, this is passed on to the Designated Safeguarding Lead and, where appropriate, the E-safety Coordinator.

Student reporting outside school

Students are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with a trusted adult such as their parents, carers, guardians or school staff.

Allegations against staff

Allegations involving staff should ordinarily be reported to the Headteacher or through the Whistleblowing Policy. If the allegation is one of abuse then it should be handled in line with the statutory DfE guidance: 'Dealing with allegations of abuse against teachers and other staff'. If necessary local authority's LADO should be informed.

Evidence of incidents must be preserved and retained and where necessary, the LADO informed.

The curriculum will cover how students should report incidents (e.g. CEOP button, trusted adult, Childline)

Appendix J: How to Manage Student Breaches of the Acceptable Use Policy

Where a student is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

Remedial action relating to potential sanctions is at the discretion of school management as suggested as below.

The following are provided as exemplification only, and should be amended and/or confirmed by the school, as appropriate:

Level 1 breaches

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other devices/technologies) in lessons, e.g. to send texts to friends
- Use of unauthorised instant messaging/social networking sites

[Possible Sanctions: refer to class teacher / e-Safety Coordinator/ confiscation of phone or other device]

Level 2 breaches

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other devices/technologies) after being warned
- Continued use of unauthorised instant messaging/social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff
- Accidentally accessing offensive material and not notifying a member of staff

[Possible Sanctions: refer to Class teacher/ E-safety Coordinator / removal of Internet access rights for a period / confiscation of phone or device / contact with parents/carers]

Level 3 breaches

- Deliberately corrupting or destroying someone's data, violating the privacy of others
- Sending an email and/or message that is regarded as harassment or of a bullying nature (cyberbullying)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: refer to Class teacher / E-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents/carers]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 breaches

- Continued sending of emails and/or messages regarded as harassment or of a bullying nature after being warned (cyberbullying)
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school, if they are related to school or any member of its community.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and collect data evidence and/or the Local Authority Human Resources team.

Appendix L: Cyberbullying: further advice and guidance

Behaviour that is classed as cyber bullying includes but is not limited to:

- **Abusive comments**, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.

- **Sharing pictures**, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.

- **Hacking** into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.

- **Creating specific websites or 'pages' on the Internet** that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.

- **Blackmail**, or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

Cyberbullying: Advice for headteachers and school staff

The Department for Education has produced non-statutory advice for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Preventing and tackling bullying: Advice for headteachers, staff and governing bodies

This document has been produced by the Department for Education to help schools take action to prevent and respond to bullying as part of their overall behaviour policy. It outlines, in one place, the Government's approach to bullying, legal obligations and the powers schools have to tackle bullying, and the principles which underpin the most effective anti-bullying strategies in schools. It also lists further resources through which school staff can access specialist information on the specific issues that they face. This includes cyberbullying.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf

Appendix M

School/academy Personal Data Advice and Guidance

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools/academies will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school/college is encouraged to seek their own legal counsel when considering their management of personal data.

The template uses the terms students/pupils to refer to the children or young people at the institution.

Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school/academy receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term "Data Protection Law" refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'.

A school/academy is, for the purposes of the Data Protection Law, a "public body" and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the Information Commissioner's Office (ICO) website including information about the Data Protection Law.

The ICO's powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to data subjects;
b) collected for specified, explicit and legitimate purposes and not further processed in a

manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school/academy to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities

The school/academy and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school/academy may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school/academy has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school/ academy, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school/academy the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors – and personal data of names, addresses, contact details
- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as '**special category**' being personal data;
"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"
This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.
The school/academy will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

(a) Consent:	the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
(b) Contract:	the processing is necessary for a contract you have with the data subject
(c) Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that *"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"* however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.
Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed

and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"
This means that where a school/academy is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools/academies should consider the capacity of pupils to freely give their informed consent.
The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:
"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."
You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.

- if your school or academy requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is
- What personal data is being processed and the lawful purpose of this processing
- where and how the personal data was sourced
- to whom the personal data may be disclosed
- how long the personal data may be retained
- data subject's rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the school/academy will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school/academy will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a school/academy context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.
A school/academy must not disclose personal data even if requested in a Subject Access Request;

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school or academy must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school/academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school/academy or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools/academies are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data

- the school/academy will want to avoid the criticism and negative publicity that could be generated by any personal data breach

Schools / academies have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school/academy but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.
Schools / Academies will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.
All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.
If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

The school/academy should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.
DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.
The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?

- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school/academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school/academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/academy personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

The school/academy will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school/academy should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school/academy systems, including off-site backups.

The school/academy should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school/academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school/academy is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.
All paper based personal data must be held in lockable storage, whether on or off site.

Appendix N: Secure transfer of data and access out of school

The school/academy recognises that personal data may be accessed by users out of school/academy or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school/academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school/academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of personal data

The school/academy should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school/academy must ensure the safe destruction of personal data when it is no longer required.
The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.
A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school/academy to target training at the most at-risk data
- record any breaches that impact on the personal data

Fee

The school/academy should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school/academy to a penalty in additional to other fines possible under the Data Protection Law.

Responsibilities

Every maintained school/academy is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks

- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law

The school/academy may also wish to appoint a Data Manager. Schools/academies are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / academy's information risk policy and risk assessment
- oversee the System Controllers

The school/academy may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school/academy has the responsibility of handling protected or sensitive data in a safe and secure manner.
Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school/academy or elsewhere if on school/academy business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school/academy to consider whether the requested information should be released into the public domain. FOI links to Data Protection Law whenever a request includes personal data. Good advice would encourage the school/academy to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/academy's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school/academy to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's / academy's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / academies complete the Guide to Information for Schools.

Parental permission for use of cloud hosted services

Schools/academies that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools/academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools/academies under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Law
- They must provide alternative means for accessing services where a parent or pupil has refused consent

New advice to schools/academies makes it clear that they are not able to use pupils' biometric data without parental consent. Schools/academies may wish to incorporate the parental

permission procedures into revised consent processes. (see Appendix Parent / Carer Acceptable Use Agreement)

Privacy and Electronic Communications
Schools/academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Appendix O: School/academy policy template: Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil/student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.
The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.
Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).
An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
The *Head Teacher/Principal* must publicise the school behaviour policy, in writing, to staff, parents/carers and students/pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).
DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" (2014 and updated January 2018)

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The *Headteacher/Principal* is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher/Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Simon Iddon DSL

The *Headteacher/Principal* has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: SLT and HoY in pairs and always insuring a female is present when searching a girl and vice versa.

The *Headteacher/Principal* may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training/Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher/Principal to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

Pupils/students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.
If pupils/students breach these roles: See behaviour policy

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:
The authorised member of staff must have reasonable grounds for suspecting that a *student/pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).
The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils/students.)
The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student/pupil being searched.
The authorised member of staff carrying out the search must be the same gender as the *student/pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student/pupil* being searched.
There is a limited exception to this rule: Authorised staff can carry out a search of a *student/pupil* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

Extent of the search:
The person conducting the search may not require the *student/pupil* to remove any clothing other than outer clothing.
Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
'Possessions' means any goods over which the *student/pupil* has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)
A student's/pupil's possessions can only be searched in the presence of the *student/pupil* and another member of staff, except where there is a risk that serious harm will be caused to a

person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Staff must not examine the content of any student device.

If inappropriate material is contained on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.
A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

Organisational control

Roles & Responsibilities

- **SLT**
    - Facilitating training and guidance on Social Media use.
    - Developing and implementing the Social Media policy
    - Taking a lead role in investigating any reported incidents.
    - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
    - Receive completed applications for Social Media accounts
    - Approve account creation
- **Administrator/Moderator**
    - Create the account following SLT approval
    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies

- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school/academy accounts
- Adding an appropriate disclaimer to personal accounts when naming the school/academy
-

Process for creating new accounts

The school/academy community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school/academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/academy, including volunteers or parents.

Monitoring

School/academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school/academy social media account.

Behaviour

- **The school/academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School/academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school/academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school/academy media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely

seriously by the school/academy and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school/academy policies. *The school/academy permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school/academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/academy will deal with the matter internally. Where conduct is considered illegal, the school/academy will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school/academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school/academy protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)
-

Use of images

School/academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's/academy's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student/pupil pictures online other than via school/academy owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Students/pupils should be

appropriately dressed, not be subject to ridicule and must not be on any school/academy list of children whose images must not be published.

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
  - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
  - Personal communications which do not refer to or impact upon the school/academy are outside the scope of this policy.
  - Where excessive personal use of social media in school/academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
  - *The school/academy permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
  - **Staff are not permitted to follow or engage with current or prior pupils/students of the school/academy on any personal social media network account.**
  - The school's/academy's education programme should enable the pupils/students to be safe and responsible users of social media.
  - Pupils/students are encouraged to comment or post appropriately about the school/academy. Any offensive or inappropriate comments will be resolved by the use of the school's/academy's behaviour policy
- **Parents/Carers**
  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - The school/academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school/academy. In the event of any offensive or inappropriate comments being made, the school/academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's/academy's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school/academy.
- The school/academy should effectively respond to social media comments made by others according to a defined policy or process.

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school/academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school/academy social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances