SPALDING HIGH SCHOOL

PERSONAL ELECTRONIC DEVICES, MOBILE PHONE & SOCIAL MEDIA POLICY

HEADMISTRESS:		**Mrs M K ANDERSON**
LINK GOVERNOR:	**(SEND)**	**Mrs D MULLEY**
	(SAFEGUARDING)	**Mr E FRAGALE**
	(HEALTH & SAFETY)	**Mr J SMITH**
DATE AGREED		**June 2019**

Executive Summary:

This policy sets out the use of personal electronic devices, including mobile phones at Spalding High School. It also details our work and approach to the use of social media and social networking.

Review Date: June 2021

Links to related policies:
Behaviour for Learning Policy
Child Protection & Safeguarding Policy
Student Acceptable Use Policy
Staff Acceptable Use Policy
Safeguarding Policy
Photographic & Image Consent

_____ _____

Chairman of Governors **Date**

_____ _____

Headmistress **Date**

Section 1: Rationale

1.1 Safeguarding is the prime concern underpinning our electronic device, mobile phone and social networking policy.

1.2 As a School we understand, appreciate and encourage the digital world that our young people are growing up in. We also understand that in extreme cases, electronic devices, mobile phones and social media can be used to disrupt learning, invade privacy, bully, intimidate, threaten and humiliate. We have a duty of care to our students, our staff and our School and will uphold the appropriate use of technology but will deal will those who break our rules and place us at risk.

1.3 For the purposes of this policy "in school" includes the entire grounds of the School within the perimeter boundary fence, as well as offsite school approved trips and activities.

1.4 Staff should not be questioned or challenged about these rules. Any student doing so will be dealt with by senior staff.

1.5 From February 2014 Ministers gave schools the right to search, screen and confiscate personal mobile devices.

Section 2: Personal Electronic Devices

2.1 For the purposes of this policy, personal electronic devices (PED) refers to all technology such as mobile phones, tablets, e-readers, cameras, music devices, recording equipment etc. irrespective of brand name, generation, or type.

2.2 **ALL** such items **MUST** be locked in student lockers during the school day. There are only two exceptions to this rule:

- If a member of staff allows students to use their PED for a specific learning activity within their lesson and under their direct supervision.
- Sixth Form students may **discreetly** use their mobile phones and PED in the common room and sixth form area (not around site.) If a member of staff requests a student to put their phone or PED away they must comply.

2.3 The School is not responsible for loss, damage or theft of PED and parents are advised to arrange suitable insurance should they allow their child to bring such items to school (including school trips and visits). However, if an item is stolen, the School will make a reasonable attempt to investigate the theft and recover the item. This may involve the theft being reported to the police.

2.4 No PED is to be charged in school.

Section 3: Wi-Fi & Internet access

See Appendix 1: Student Acceptable Use Agreement

3.1 **NO** PED (including mobile phones) are to be connected to the School system, wi-fi or internet. Students should remember that they have all signed an Acceptable Use Policy which specifies the use of technology and school systems.

Section 4: Mobile Phones

4.1 No student needs their phone with them during the school day unless they have been asked to use it as a learning tool by a teacher (see point 2.2 (a) above).

4.2 In the case of a genuine emergency a student should report to the school reception at (preferably) break, lunch or after school to speak to their parent/carer on the school land line.

4.3 Should a parent/carer need to contact their child in an emergency they should call the school reception and not their child on their mobile phone.

4.4 Mobile phones are permitted on site but must be switched off upon entry to the school site and not be switched on again until students prepare to leave the school at 3.45pm. (See exceptions 2.2 (a) & (b) above). We recognise that as students prepare to leave school at 3.45pm they may text/call their parents that they are beginning their journey home. This is acceptable but students must be vigilant to site & road dangers such as moving vehicles on the drive and car park areas. They must not wear earplugs in these hazardous areas and must remain vigilant to hazards if walking and calling/texting.

4.5 All mobile phones must be locked in lockers during the day (see exceptions 2.2 (a) & (b) above). Having the phone switched to silent mode and being carried around is **not** acceptable and will be viewed as a breach of the rules.

4.6 If a student is found in possession of a mobile phone (switched on or off, being used, or not) it will be confiscated by the member of staff, handed in to the school office with the student's name and the student placed in detention. A letter will be sent home informing parents/carers of the contravention of school rules and the confiscation of the mobile phone.

4.7 The student should report to the Headmistress at the end of the timetabled day (3.40pm) to discuss the contravention of school rules and the confiscation of the phone. Following this discussion the phone will be returned to the student (on the first occasion).

4.8 Should the confiscation occur for a second time, the student will be required to hand their phone in at reception in the morning and then collect it at the end of the day, for two weeks.

4.9 Should a further incidents of confiscation occur then appropriate action will be taken.

4.10 In certain after school events such as fixtures, trips or students working in the library, and with permission from the staff in attendance, students may use their mobile phone to contact parents to arrange pick-ups.

Section 5: Smart watches

5.1 A basic time piece is all that is required by a child at school. However, should a student wish to wear a smart watch to school then all obvious elements of this policy apply to the watch and its use must be limited solely to time keeping. The smart watch must **not** be used to access the internet, social media or the School wi-fi during the School day.

5.2 No smart watch or wristwatch with a data storage device is permitted in a test room or examination venue. The wearer will have to remove it and secure it in their locker.

Section 6: PEDs, recordings and photographic images
See Appendix 2 Photographic and Image Consent Form

6.1 No PED may be used as a recording device or camera without the express permission of those being recorded or photographed.

6.2 Images and recordings are within the remit of the School's Photographic and Image Consent and are for private use and private storage only. Such images, recordings or films are prohibited from being shared on-line without the consent of **ALL** of those with parental responsibility for **EACH** child appearing in the images or recordings. Such images or recordings must be kept securely and may be for personal use only.

Section 7: Social Media and networking

7.1 All students have signed an Acceptable Use Policy which details use of school systems, technology and networks. They also receive guidance and education on E-Safety through our PSHCE programme, Computing lessons and specific events over the course of the academic year.

7.2 E-Safety is also a community focus in our Curriculum Evenings for parents. We have developed an area of the School website with advice and links for parents and students. (Students/Pastoral care)

7.3 The School is not responsible for pupils' online activity outside of school. Parents have responsibility for their child's online behaviour and digital footprint outside of school and are advised to ensure that privacy is set to the securest level and online behaviour is legal and appropriate.

7.4 However, should the School receive evidence that any comment, image or recording judged by us to be inflammatory, threatening, malicious, offensive or inappropriate about a named pupil, member of staff or the School itself be placed within the public domain then action will be taken. This action may include a formal report or complaint to the police.

7.5 If a student is feeling concerned, they should:

- Not delete anything – keep everything – it may be needed as evidence.
- Tell someone - Inform parents/carers/staff of what is happening.
- Use the service provider's website to report the incident.
- Block the perpetrator.

- In incidents of malicious or inappropriate communication follow the police procedures (see CEOP website for details.)

7.6 Students should keep safe online by:

- Only adding people they know in the "real" world to their friends list and sites.
- Keep their password safe and change it regularly.
- Think carefully about what they post, send and share – once it is online it is there forever and anyone can use it.
- Use the CEOP and ThinkUknow websites and what they have learnt in school to stay safe online
- Engage with their parents- they are not being nosey – they want their child to be safe.

Section 8: Examinations and Test situations

8.1 **NO** PED is to be taken into an examination venue or test situation. If a candidate forgets they have a PED on their person, it must be surrendered to the lead invigilator.

8.2 Contravention of this point could result in a student being reported to an examination board for misconduct. This could, in extreme cases, result in the banning from examinations or loss of grades/awards.

8.3 The School upholds the Joint Council for Qualifications ruling of: "no ipods, smartwatches or wristwatches with a data storage device, mobile phones, MP3/4 players; no potential technological/web enabled sources of information; possession of unauthorised items, such as a mobile phone, is a serious offence and could result in disqualification from your examination and your overall qualification."

8.4 The School shares and upholds the JCQ 'information for candidates using social media and examinations/assessments' – to guide candidates to stay within the examination regulations.

Section 9: Staff and Visitors

See Appendix 3 Staff Acceptable Use Policy

9.1 All staff have signed an Acceptable Use Policy and are subject to the School's Safeguarding policy.

9.2 Teaching staff are expected to have their PEDs (inc mobile phones) turned off during lessons unless it is being used for a learning activity.

9.3 The only phone in an examination venue is held by the lead invigilator for emergency purposes.

9.4 Support staff, visitors and teaching staff (when not teaching) may have their mobile phones switched on but they must be on silent.

9.5 Text messages should not be read or sent nor calls made or received during lessons.

9.6 Recordings and photographic images of students must not be kept on staff PEDs (inc. mobile phones).

Section 10: Advice and Guidance

10.1 The School is always willing to listen and try to help resolve issues. Students and parents are welcome to contact any member of staff they feel comfortable talking to. However, our Pastoral Team have the most experience in these areas.

10.2 Alternatively, parents who are concerned about their child's use of PEDs, social media or digital/cyber bullying may find the following websites useful:

- www.anti-bullyingalliance.org.uk
- www.ceop.gov.uk
- www.childline.org.uk
- www.kidscape.org.uk
- www.nspcc.org.uk
- www.thinkuknow.co.uk
- https://www.saferinternet.org.uk

APPENDIX 1

Spalding High School

Acceptable Use Agreement

Introduction

Please read this "Acceptable Use" document carefully. It is designed to explain the use of Computer Networks within Spalding High School and the responsibilities that you as a student are required to observe, in its use. This Acceptable Use Agreement is underpinned and supported by both the School's Behaviour Policy and Personal Electronic Devices and Mobile Phone Policy. Students and Parents should read both policies in full on the school website.

Scope

The following rules and procedures have been formulated to ensure a clear understanding of the responsibilities in the use of the school computer system, e-mail and Internet facilities and applies to all students.

It applies to all computer software and hardware provided by the school including Personal Computers, Laptops, Wireless & Broadband connections, Servers and any other equipment that may be provided for use and for Special Educational Needs.

In reference to the School's Personal Electronic Devices (PED), Mobile Phone and Social Media Policy; No PED is to be charged in school. No PED (including mobile phones) are to be connected to the school system, wi-fi or Internet. Students should remember that they have all signed an Acceptable Use Policy which specifies the use of technology and school systems.

Email and Internet

- The email and Internet system is provided for education purposes only and should not be used for personal gain or reward.

- Sending messages of an abusive, offensive, harassing, racist, discriminatory or obscene nature is not permitted and will result in disciplinary action which may include withdrawal of access rights. Should the school receive evidence that any comment, image or recording judged by us to be inflammatory, threatening, malicious or offensive about a named pupil, member of staff or the school itself be placed in the public domain, then action will be taken. This action may include a formal report or complaint to the police.

- Access to the Internet is restricted and filtered on content and is available for suitable educational requirements. Accessing or attempting to access, downloading and/or uploading abusive, offensive, obscene or illegal material is strictly forbidden and pupils must follow guidelines from teachers in lessons where access to online digital resources (e.g. webpages and YouTube content) are being used to enhance teaching and learning.

- It is important that care should be taken when downloading material from the Internet that copyright notices and license implications are observed.

- Personal use of email and the Internet is permitted, provided it is carried out in the student's own time, during non contact periods (Sixth Form), out of normal school hours, or by prior arrangement with a member of staff.

Cyberbullying

- Cyberbullying is the sending or posting of harmful or cruel text messages and/or images, using the Internet or other digital communication devices.

- Spalding High School does not tolerate bullying in any form. Any student found to be involved in incidents of cyberbullying will be dealt with firmly.

- The School Behaviour Policy and Personal Electronic Devices, Mobile Phone and Social Media Policy sets out clearly the procedures and sanctions available to staff to deal with incidents of cyberbullying.

Monitoring

- The school maintains security and anti-virus software that monitors and records details of all network activity in which individuals transmit or receive files and data.

- To ensure that the rules and procedures are being followed, both email and Internet use will be monitored on a regular basis. This will include the access of Internet sites and email sent or received though school servers.

Security and Confidentiality

- Every user will be issued with a unique user name and password; this must be **kept confidential**, not written down or given to others. The password should be changed on a regular basis in accordance with the system default password expiry period.

- Each user will have their own area on the network for the storage of data files, coursework and email. The IT Manager and associated staff will at times randomly inspect data stored on the school networks to check appropriate content of such data.

- Screens should never be left unattended and after use, all computers should be logged off from the network.

- For personal safety, any form of electronic communication should have no references to personal information such as student home addresses, telephone numbers etc.

- It is the responsibility of all students to protect the security and confidentiality of the school networks. Students must not try to deliberately access the online files and folders of their peers, teachers or others.

Failure to abide by this policy on acceptable use will result in disciplinary action, which may include withdrawal of access rights. In serious cases it may result in legal action.

You are now requested to sign your acceptance of this policy and agreement document. This has been provided in the form of a separate page accompanying this document, such that the student can **keep the actual policy for reference** and the signed portion can be filed with student records for future use. A summary of this policy can also be found in the school planner.

APPENDIX 2

Spalding High School

Photographic and image Consent Form

Occasionally, we may take photographs of the pupils in our School. We may use these images in the School Prospectus or in other printed publications that we produce, as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use. Sometimes contracted outside agencies such as trip venues or activity organisers may take photographs of our pupils participating in one of their activities.

From time to time, the School may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may be printed in local or national newspapers, or be on televised news programmes.

To comply with the Data Protection Act (1998), Taking Photographs in Schools (2014) and the GDPR 2018 regulations we need your permission before we can photograph or make any recordings of your child. The School observes the County Council's guidelines on the use of photographs and electronic images in Schools (March 2015). Please answer questions 1 to 5, read the declaration and sign and date the form below:

		Please circle your answer
1	May we use your child's photograph (unidentified) in the School Prospectus and other printed publications that we produce for promotional purposes?	Yes / No
2	May we use your child's image (unidentified) on our website?	Yes / No
3	May we record your child's image (unidentified) on video or webcam?	Yes / No
4	Do you consent to your child being photographed or filmed in press events/by contracted outside agencies if agreed by the School?	Yes / No
5	Do you consent to your child's full name being published with a press photograph? (At the present time, local newspapers will not agree to publish a photograph in print or on their internet newspaper without a full name).	Yes / No

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

"Unidentified" above means we will use either no name or first name only.

Parents may take photographs and film activities ONLY for personal use. The Data Protection Act does not prohibit parents, friends and family members from taking photographs of their child and friends participating in school activities for the family album and they may film activities at school to watch at home. Such images or films taken by parents are prohibited from being shared on-line without the consent of all of those with parental responsibility for each child appearing in the images. Parents must keep their photographs and films securely and may only share with family members for personal use.

I understand that the School will destroy electronic and actual photographs of my child when they leave the School, although important photographs will be retained for the school archive.

I have read and understood the conditions of use on this form.

Student name …….. Form ……..

Parent/Carer Signature …… Date ……

Name (in block capitals) ……..

APPENDIX 3

SPALDING HIGH SCHOOL

STAFF ACCEPTABLE USE POLICY

HEADMISTRESS:	**Mrs M K ANDERSON**
IT MANAGER:	**Mr J SMITH**
DESIGNATED SAFEGUARDING LEAD (DSL):	**Mrs L RAY**
DEPUTY DSL:	**Mrs A SCHWARZ**
LINK GOVERNOR:	**Mr J SMITH (H&S)**
	Mr E FRAGALE (SAFEGUARDING)
DATE AGREED:	**June 2017**
REVIEW FREQUENCY:	**Biennial**

Executive Summary:

The aim of this policy is to set out the individual responsibilities which assist in protecting Spalding High School (SHS) and by association, the Local Authority (LCC) information, data, systems, pupil and staff safeguarding. Full credit is given to Lincolnshire County Council (LCC) Information Security Policy Framework (2015) and the LCC Acceptable Use Policy.

As a professional organisation with responsibility for children's safeguarding all users of our facilities, systems and information have a responsibility to use them in a professional, lawful, and ethical manner. In addition, it is vital that users of our facilities, systems and information take all possible and necessary measures to protect against infection, unauthorised access, damage, loss, abuse, misuse and theft.

School facilities, systems and information must not be used in any way that could be damaging to Spalding High School's public image, or for purposes not in the interest of the School, or is abusive, offensive, defamatory, obscene or indecent or of such a nature as to bring the School, the Local Authority or its staff and pupils into disrepute.

This Acceptable Use Policy applies to individual's using or accessing School IT equipment, information or systems. This includes, but is not limited to, employees, governors, contractors, consultants, volunteers, and third party organisations. It applies to all School owned or leased IT including computer equipment, smart & mobile phones, software, Internet/Intranet related services, operating systems, storage media and access to network resources. This policy does not contain exhaustive lists and all users are reminded that IT use should be consistent with the School ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

The statements in this policy are designed to ensure that colleagues are aware of the acceptable use of IT and their responsibilities to protect and secure all council or school owned information systems, computer equipment, accessories and data. To ensure that members of staff are fully aware of their professional responsibilities when using Information Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

Related Policies:
Safeguarding Policy
Photographic & Image Consent Form
Personal Electronic Device, Mobile Phone, Social Media Policy (Pupils)
Student Acceptable Use Policy

_____ _____

Chair of Governors **Date**

_____ _____

Headmistress **Date**

Section 1: Protecting data

1.1 Users must only process personal data if they have a justified business (school based) reason and they are authorised to do so.

1.2 Users must ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN).

1.3 Any pupil (or staff) sensitive data that is removed from the School site should only be removed via the encrypted memory stick. Normal resources & work does not need to be removed via encrypted files on a USB.

1.4 Any images or videos of pupils must only be taken and used as stated in the School's Photographic and Image Consent Form (Appendix 1) and will always take into account parental consent.

1.5 Users must not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted.

1.6 Users must protect the devices in their care from unapproved access or theft.

1.7 Users must respect copyright and intellectual property rights at all times.

Section 2: Monitoring

2.1 Use of the computer systems and data provided by the School will be subject to monitoring for security and/or network management reasons. Monitored systems include, but are not limited to, Internet/Intranet, email and Office applications.

2.2 The School reserves the right to monitor or record all communication systems, including email, electronic messaging and internet use. Records of activity may be used by the organisation for the following purposes; quality assurance; conduct; discipline; performance; capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislative framework in force and useful to support the School's business activities. The School reserves the right to determine the suitability of this information.

Section 3: Breaches of Policy

3.1 All school and council employees have a contractual responsibility to be aware of and conform to the School and Council's values, rules, policies and procedures. Breaches of policy may lead to the employee becoming the subject of school or council based disciplinary procedures in accordance with the Code of Conduct and the Disciplinary Policy and Procedure.

3.2 Individuals who are not council or school employees but fail to comply with this policy may have their school or council information and/or IT revoked and such action could have impacts on contracts with third party organisations.

Section 4: Training and awareness

4.1 The School will provide training to equip staff with the necessary skills and knowledge to both meet the School's needs and provide safeguarding duty of care to staff and students.

4.2 Staff IT training may be provided to cover statutory requirements or the needs of departments or individuals. Sessions can also be tailored to meet the needs of the School and the requirements of individuals. Where new software and applications are introduced to the School, specific sessions will be planned to take account of this. Help sheets and 'how to' guides will be provided where required. Users should familiarise themselves with documentation provided for training and information.

4.4 Where IT training is linked to safeguarding issues, it will be provided as part of the School's safeguarding training cycle via the first training day in September and subsequent twilight or training slots thereafter according to the published programme.

4.5 Training will be provided either for the whole staff, smaller groups, or on a one-to-one basis.

4.6 Staff should discuss any training requirements they feel may be required to fulfil their duties with their line manager.

Section 5: Internet and E-mail

Please See Appendix 2 for detailed guidelines/etiquette for use of the E-Mail and Sims messaging systems at SHS
See Appendix 3 for notes about staff use of YouTube

5.1 The Internet is to be used in a manner that is consistent with the School's ethos and code of conduct and as part of normal execution of a staff member's job responsibilities.

5.2 The distribution of any information through the Internet, computer-based services, email and messaging systems is subject to the scrutiny of the Headmistress.

5.3 Electronic communications with pupils, parents/carers and other professionals must only take place within clear and explicit professional boundaries and must be transparent and open to scrutiny at all times. All communication must take place via a school approved channels and not via personal devices or accounts.

5.4 Any pre-existing relationships or situations that may compromise this (5.3) should be discussed with the Headmistress or Designated Safeguarding Lead immediately that it arises.

5.5 Users must check that the recipients of email messages are correct so that personal or sensitive information or data is not accidentally released into the public domain.

5.6 Personally owned email accounts must not be used to transmit or receive school or council information. If staff are transmitting school or council information it should either be via the school email system (accessed via the internet if off the premises) or via the encrypted memory stick.

Section 6: Security

6.1 Access levels to the computer systems, user identifications and password systems will be set and managed by the IT Manager in consultation with the Deputy Headteacher.

6.2 Users are thereafter, responsible for their user name and password or other mechanism as provided (eg access tokens), and must protect their user credentials against misuse.

6.3 Users must never disclose their user identities or passwords to another person. They should ensure that their passwords are strong and are changed regularly and should not write down passwords in locations where they are easily accessed. It is advised that if possible passwords are not written down at all.

6.4 Forgotten passwords will be reset only by the IT Manager.

6.5 Users must not use the credentials of another person to access IT.

6.6 Users must ensure that they log out of the system after use and do not leave the computer or device unattended whilst it is still logged into the system. The computer can be left unattended and logged on for short periods of time, but in those circumstances it must be locked using the 'Lock this computer' facility.

6.7 Users must seek to prevent inadvertent disclosure of personal or sensitive information by; avoiding being overlooked when working; by taking care when printing information; and by carefully checking the distribution list for any material to be transmitted.

6.8 Users must not give individuals from outside the school access to the School's computer systems. This includes, but is not limited to, allowing family members or friends' access to school computer equipment.

6.9 Users must not send personal or sensitive information or data over public networks such as the internet unless an approved method of encryption has been applied to it.

6.10 Users must only access or attempt to access IT or information that they have been given permission to access. If users believe they have been provided with access to IT or data in error, they must stop any activity and report their concerns to the IT Manager or Headmistress immediately.

6.11 Users must not misuse the configuration or settings of any IT.

6.12 Users must not attempt to bypass or subvert IT security controls.

6.13 Users must not download software programmes for use on the network without authorisation from the IT Manager. Documents & files downloaded must be for business use only. Deliberate unauthorised access to, copying, alteration, or interference with school computer applications or data is not allowed.

6.14 All computer applications and data developed for the School are for the sole use of the school except by permission of the Headmistress.

6.15 Users must ensure that data held on removable media is securely erased or the media is destroyed when no longer required.

6.16 All staff are required to report violations of the security procedures established within this policy directly to the IT Manager immediately who will work with Line Managers and the SLT to resolve/address the problem.

6.17 Any alteration to the data of other staff without their explicit authorisation is prohibited.

6.18 Attempts to hack into the network or enabling the malicious introduction of viruses, Trojans etc contravenes the Computer Misuse Act 1990 and will be dealt with as such.

Section 7: Computer & IT Equipment

7.1 The acquisition and utilisation of computer equipment and software requires the approval of the IT Manager in order to ensure system compatibility and compliance with the IT strategy of SHS.

7.2 All computer equipment must be kept in a secure location.

7.3 Only Network Support and site staff are permitted to move desktop computers and printers. Users must not move these items and should notify Network Support if an item requires movement to a new location so that current Health and Safety requirements and network compatibility is met.

7.4 No personal computer hardware or personal electronic device (P.E.D) is to be connected to the School's network without prior permission of the IT Manager.

7.5 It is the responsibility of the user of portable equipment to ensure its security at all times. This requires the user of portable equipment to ensure:

- It is locked away and out of sight when not in use;
- It is secured whilst in use and left unattended temporarily (e.g. laptop security cable or similar);
- That equipment is not left unattended in a vehicle. If a user does have to leave the equipment unattended in an emergency, it must be securely locked away in the boot of their car;
- Equipment must never be left visible in a vehicle, even when the vehicle is occupied.

7.6 Users are responsible for all portable equipment and accessories issued to them and are required to look after, transport and store the equipment effectively in order to prevent damage to the equipment and accessories. Levels of damage/loss will be monitored and reported to the Headmistress.

7.7 Users are only permitted to use the portable equipment of the School that is issued to and signed for by them, and thereby authorised for their professional use.

7.8 Persons leaving the employment of the School must return all portable computer equipment and accessories before departure.

7.9 The disposal of computer equipment requires the approval of the IT Manager in order to ensure asset replacement and disposal procedure compliance.

Section 8: Personal Electronic Devices (PEDs)

8.1 Staff with permission to connect their personal electronic devices (of *any* kind) to the School's wireless network accept that, where appropriate, they must comply with the requirements and terms of this policy.

8.2 Staff incorporating P.E.D items as part of an IT enriched curriculum must be familiar with, and ensure that both they and their pupils abide by all aspects of the School's P.E.D policy.

8.3 The School is not responsible for loss, damage or theft of P.E.D and colleagues are advised to arrange suitable insurance should they bring such items to school (including school trips and visits.) However, if an item is stolen, the School will take a reasonable approach to investigating the theft and to recover the item. This may involve the theft being reported to the police.

Section 9: Computer System Storage and Usage

9.1 Data stored on the local hard disk (e.g. *C:\ or D:\ drive*) of portable equipment cannot be backed up from the network and it is therefore the responsibility of the individual to make regular backups.

9.2 All school data should be saved to the school network *(e.g. T:\ drive)* where it can be regularly backed up.

9.3 Users should ensure they do not use external storage devices as a long term storage medium for their school data. External storage should only be used to transfer data from one location to another *(e.g. home to school)* where the use of the computer network and/or Internet is not possible *(or practical)*. External storage devices are easily lost, stolen and the contents corrupted. As these devices do not connect to the School's computer network we are unable to recover any lost data.

9.4 No sensitive data including, but not limited to, information about students *(e.g. class lists, registers and reports)*, should ever be saved to an unencrypted external storage device as this contravenes the Data Protection Act 1998. Please see point 1.3 above.

9.5 System storage space is finite and users should routinely remove or archive old files from the school networked systems *(i.e, T:\ drive, S:\ drive and L:\ drive)*. Failure to do so may result in a user being unable to save their work, or in the worst case, account failure.

9.6 E-mail and SIMs messaging storage space is finite and users should routinely remove or archive messages from their Inbox (including any subfolders), Sent Items and Deleted Items. Failure to do so will result in the user being unable to send or receive e-mails/SIMs messages.

Section 10: Unacceptable use and the potential to cause offence

10.1 Users must not create, transmit, display, publish or forward any material that is likely to harass, incite, cause offence, inconvenience or needless anxiety to any other person or group, or anything which could bring their professional role, the School, or the County Council, into disrepute.

10.2 Users must not process, access, store or display any racist, extremist, hate related, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material. Nor may they carry out activities that are illegal, fraudulent or malicious on any school or council owned systems, hardware or equipment.

10.3 Users must not annoy or harass other individuals or groups for instance by sending chain letters, uninvited emails of a personal nature or by using lewd or offensive language.

10.4 Users must ensure that their online reputation and use of IT and information systems are compatible with their professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. Users must recognise that their digital and on-line presence may be viewed as reflective of Spalding High School and must ensure that professional distance and reputation are maintained.

10.5 Users must take appropriate steps to protect themselves online and will ensure that their use of IT and internet will not undermine their professional role, interfere with their work duties and will be in accordance with this policy and the law.

Section 11: Personal Use

11.1 Personal use of School systems such as the internet or email should be reasonable, proportionate and occasional and must not interfere with the performance of the user's role, time management or performance of the systems.

11.2 School IT facilities are there to support our School. The Headmistress chooses to permit limited personal use as long as this does not conflict or interfere with normal school activities or have a financial cost to the School.

11.3 Any such personal use must comply with all the requirements and terms of this policy.

11.4 Personal use will only be authorised for the user; it shall not be extended to any other person. This includes, but is not restricted to, family members or friends.

11.5 The personal use of social networking websites such as, but not limited to, Facebook and Twitter is prohibited on all School owned equipment and systems unless authorisation have been given by the Headmistress.

11.6 The personal use of any site blocked by the School's network on school owned equipment (kept in school or at home) is prohibited.

11.7 Users must not store any personal information on the School computer systems and equipment (including any school laptop or similar device issued to staff) that is unrelated to school activities, such as personal photographs, music, files or financial information. School printers should not be used for personal printing. Any such stored media will be removed by the IT Manager in consultation with the user.

Section 12: Safeguarding

12.1 Safeguarding permeates all aspects of this Acceptable Use Policy however additional key points need to be made clear:

- Users must report all incidents of concern regarding children's online safety or well-being to the Designated Safeguarding Lead as soon as possible;
- Users must report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead as soon as possible;
- Users must promote online safety with the pupils in their care and must help them to develop a responsible attitude to safety online, system use and to the content they access or create;

If users have any queries, concerns or questions regarding safe and professional practice electronically or online either in school or off site, then they must raise them with the Designated Safeguarding Lead or Headmistress as soon as possible.