The Dales School
North Yorkshire

# Information Communication Technology (ICT), Social Media and E-Safety Policy

| | |
|---|---|
| **Person Responsible:** | Headteacher |
| **Reviewed by the School:** | February 2022 |
| **Approved by the Full Governing Body:** | February 2022 |
| **Next Review Date:** | February 2023 |

**Signed**…………………………………………... **Date**:

# The Dales School
# Information Communication Technology (ICT), social media and E-Safety Policy

**Scope of the Policy**
This policy applies to all members of school (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

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. 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents' carers of incidents of inappropriate Online Safety behaviour that take place out of school.

This policy links with the Schools:

- Safeguarding policy and reporting procedures.
- Code of Conduct Policy.
- Behaviour policy.
- Information Policy.
- Whistleblowing Policy.

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant roles named in the policy will be effective in carrying out their online safety responsibilities in full collaboration with all polices named above and with particular compliance with the safeguarding policy.

**Roles and Responsibilities**
The following section outlines the online safety roles and responsibilities of individuals and groups within the school and also how this will be applied:

**Governors**:
Governors are responsible for the approval of this Policy and for reviewing the effectiveness of the policy; to enable this Governors will receive regular information about online safety incidents and monitoring reports. The Designated Safeguarding Governor role will also include Online Safety. The role of the Online Safety Governor will include:

- regular monitoring of online safety incident logs
- reporting to relevant Governors meeting

Governors should take part in online safety training/awareness sessions, with importance for those who are members of any subcommittee/group involved in technology/online, safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. South West Grid for Learning (SWGfL)).

- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

**Headteacher and Senior Leaders:**
The Headteacher and Deputy Headteacher are the Schools Designated Safeguarding Leads and as such take on responsibility of online safety Coordinators and have the following responsibilities:

1. A duty of care for ensuring the e-safety (including online safety) of members of the school community.
2. Are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (Appendix 1 "Responding to incidents of misuse" and relevant Local Authority HR/other relevant body disciplinary procedures). For reviewing the school online safety policies/documents and ensuring that the school meets the required online safety technical requirements and any LA guidance that may apply.~~.~~
3. For ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
4. For providing training and advice for staff.
5. For liaison with the Local Authority/relevant body.
6. Liaison with school technical staff.
7. For receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments.

8. Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs.

Designated Safeguarding Leads should be trained in Online Safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

1. Sharing of personal data.
2. Access to illegal/inappropriate materials.
3. Inappropriate on-line contact with adults/strangers.
4. Potential or actual incidents of grooming.
5. Cyber-bullying.

**The School Buys in Support from Coorecom who is responsible for ensuring:**

1. That the school's technical infrastructure is secure and not open to misuse or malicious routers, wireless systems, firewalls, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school system and data. These are tested regularly, and a log of these tests maintained. The school infrastructure and individual workstations are protected by up-to-date virus software.
2. That users may only access the networks and devices through a properly enforced password protection policy.
3. The filtering policy (appendix 2) is applied and updated on a regular basis and that it's implementation is not the sole responsibility of any single person. Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
4. That monitoring/software systems are implemented and updated.
5. The software license logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
6. That servers, wireless systems and caballing but be securely located and physical access restricted.

**Admin staff are responsible for:**

1. That all users have clearly defined access rights to school technical systems and devices.
2. That email and log on accounts are created as instructed by LMT.
3. That they induct staff on email and online rules and make them aware of this policy.

**Teaching and Support Staff are responsible for ensuring that**:

1. They have signed (and will continue to sign annually), to say that they have read, understood and will comply with this policy and their GDPR responsibilities.
2. They report any suspected misuse or problem to the LMT for investigation/action/sanction
3. Online safety best practice and learning apps are embedded in all aspects of the curriculum and other activities.
4. Where applicable, students/pupils understand and follow the Online Safety Policy and acceptable use policies.
5. Where applicable, students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
6. They manage the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
7. In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
8. Students are encouraged and supported and followed to report incidents of sexting or cyberbullying both in house and via CEOPs (Child Exploitation and Online Protection) as appropriate.
9. Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
10. All digital communications with pupils/students, parents/carers should be on a professional level and only carried out using school systems.

**E-safety**

It is essential that all staff receive and practice online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- LMT will provide advice/guidance/training to individuals as required. Online Safety BOOST includes an array of presentation resources that the Online Safety coordinator can access to deliver to staff **(**https://boost.swgfl.org.uk/).

**Students/Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students/pupils to take a responsible approach. The education of students/pupils in online safety is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Children with special needs can benefit from using the internet as much as any other child. It can motivate them, help them be creative and open up new ways of communicating. Every child needs to know how to stay safe online, but for those with Special Educational Needs and Disabilities this can be more challenging, for example:

1. They may not understand subtle language and interpret it literally.
2. They may be over trusting.

3. They may not really understand the concept of friendship.
4. They may share too much personal information.
5. Their own behaviour may be interpreted wrongly by another child.
6. They may have little or no concept of personal safety.

Students/Pupils, where appropriate will be supported to:

1. Develop an awareness and capacity to show responsibility for using the school digital technology systems in accordance with this policy.
2. Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
3. Know and understand policies on the use of mobile devices and digital devices. They should also know and understand policies on the taking/use of images and on cyber-bullying.
4. Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy includes their actions out of school.
5. Bespoke and personalised responses related to students' cognition and language levels.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:
A planned online safety curriculum should be provided as part of Computing/PSHSE/other lessons and should be regularly revisited and reinforced to consolidate PSHCE learning

1. Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
2. Where appropriate students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
3. Where appropriate students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
4. Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Schools have additional duties, under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
5. Students/pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
6. Staff should act as good role models in their use of digital technologies the internet and mobile devices
7. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
8. Where pupils/students are allowed to freely search the internet, staff should be vigilant in monitoring the content of websites the young people visit.

**Communication Aids:**
Some users of these devices will not be able to toggle between different apps and will not access the camera or internet unsupervised; another group will discover how to toggle between apps and accessories but may not understand how to use them effectively. The following restrictions should be applied to every device:

1. Setting age restriction for apps
2. Setting age restrictions for internet content
3. Locking location services (an anti-theft and loss feature)
4. Restricting explicit language

The following restrictions are possible and should be made only if and when needed:

1. Disabling the camera
2. Restricting internet access
3. Restricting installing and deleting apps
4. Preventing adding ‘friends’
5. Preventing in-app purchases
6. Restricting social networking sites eg Twitter and Facebook

Every pupil and family issued with a device that enables them to access to the internet must receive e-safety training as appropriate for their age and ability and based on the work of CEOP and be aware of this policy.

Where photos/names of other pupils appear on the device, permission must be sought first from those families to include their child in a peers communication device (included as part of the photo consent form, appendix 3. In addition the parents/Carers must also sign a declaration (appendix 4) to say that they will not use/duplicate the digital images and immediately report any loss of the devices/books

Staff need to be aware that some apps access cameras and as such could be used without permission to take digital images of staff and other pupils so will need to be checked for images before it is sent home with the pupil. This aspect of acceptable use of ICT equipment will be embedded in the school’s PSHCE curriculum.

**Parents/Carers**

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

1. Curriculum activities.
2. Letters, newsletters, website, Learning Platform.
3. Parents/Carers evenings/sessions.
4. High profile events/campaigns e.g. Safer Internet Day.
5. Reference to the relevant web sites/publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

1. Digital and video images taken at school events.
2. Access to parents’ sections of the website/Learning Platform and on-line student/pupil records.
3. Their children’s personal devices in the school (where this is allowed).

**Community Users**

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA and mobile phone letter before being provided with access to school systems Appendix 5.

The school will provide opportunities for local community groups/members of the community to gain from the school’s online safety knowledge and experience. This may be offered through the following:

1 Providing family learning courses in use of new digital technologies, digital literacy and online safety.
2 Online safety messages targeted towards grandparents and other relatives as well as parents.

3 The school website will provide online safety information for the wider community.
4 Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their Online Safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk).

This list is not exhaustive, and school will consider appropriate offers on a case by case basis.

**School email**

The official school email service may be regarded as safe and is monitored. Users should be aware that email communications can be monitored.

Good practice when sending e-mails:

1. Consider if email is the correct medium for that communication or if a phone call/face-to-face will be more appropriate, however emails do create an audit information trail and can be useful for that purpose.
2. Consider who needs to receive the email; only use global email addresses (eg staff@), when necessary; also consider when replying to a global email if all the recipients need to see the reply. Copying (cc) a person into emails is good practice, but by doing so it will be assumed that it for information only and unlikely to receive a response.
3. Always add a subject and where possible keep subject topic to one per email so that the recipient can easily sort through their emails.
4. Do not use text language or informal language in an official communication
5. Always spell check emails
6. Never write a whole email in capital letters; this can be interpreted as shouting
7. Do not use the urgent flag unless necessary; recipients will not respond to the urgent flag if they perceive that you use it routinely
8. When sending attachments, consider if sharing a document via OneDrive or Sharepoint is possible/more practicable. Documents shared via office 365 do not have to be encrypted and permissions can be removed.
9. Be aware that emails have the option of creating folders so that emails that need to be kept can be filed.
10. Understand retention schedules and that email content could be requested as part of subject access request, so ensure content is professional i.e. do not write anything in an email you would not want others to see.
11. When sending an email to several people, consider if the email addresses fall under GDPR (are they personal email addresses). If so, consider BCC.
12. Only use school email accounts for school business.
13. Users must immediately report to a member of LMT receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

*Inappropriate use:* The School does not permit individuals to use school email accounts to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Access to websites that contain similar content is also not permitted when obtained via school systems. Full details of what is deemed inappropriate can be found in the Acceptable Use Policy

There is no expectation that staff should check emails over weekends, evenings or school holidays, however, it is good practice to log on before coming back after a holiday to see if there has been any important information circulated; title of emails should identify the priority. If staff are not checking their emails or responding to emails over the holiday, then they should set an out of office reply.

**Mobile Technologies**

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

**Staff allocations of technology**

Staff are issued with appropriate technology to enable them to undertake their role. See appendix 6 for declaration to be completed and signed on issuing of each device.

The school identifies a personal device as any electronic device that can be used to access and process personal data, including data accessed from the Cloud through an internet connection. This includes, but it not limited to:

- Laptop/PC
- Notebook
- iPad
- Smart Phone

| | School Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | School owned and allocated to a single user | School owned for use by multiple users | Authorised device | Pupil/Student owned | Staff owned | Visitor owned |
| Allowed in school | **Yes** | **Yes** | **Yes** | Yes | Yes | Yes |
| Allowed in classroom/ teaching area | **Yes** | **Yes** | **Yes** | No | No | No |
| Internet access | Full network access | Full network access | Full network access where printing is required | No | Internet only (guest log on) | Internet only (guest log on, but must sign acceptable use policy before being issued with password) |

Use of personal devices:

1. Visitors are provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements and they are required to sign their agreement to comply upon entering the school building.
2. Personal devices brought into the school are entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school. The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home). Lockers for staff and visitors are provided for safe storage of such devices
3. The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
4. The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security; an essential requirement if used to access school email or documentation.
5. The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

6. Users are responsible for keeping their device up to date through software, security, and app updates. The device is virus protected and should not be capable of passing on infections to the network.
7. Devices must be in silent mode on the school site and on school buses.
8. Personal devices must not be used during teaching sessions, unless in exceptional circumstances that has been approved by LMT.
9. No one is permitted to use personal digital equipment to record images of pupils, including when on trips or visits. With written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and therefore misused.
10. If a visitor is presenting training and need to use a USB device, this can only be used once a satisfactory anti-virus check is conducted by or under the guidance of the Schools ICT Technician.
11. Personal devices should be connected to Wi-Fi via the guest log on only; if a secure log-in is required; a member of LMT MUST approve this prior to password is inputted into the device.

**Accessing Cloud Services on Personal Devices**

This Accessing Cloud Services on Personal Devices policy governs the use of personal devices to access the personal data held in Cloud based systems and processed by the school.

The policies apply to all personal data and any operational data that is classified as ‘sensitive or confidential’ that is held in in one of the school’s systems and accessed through a non-school provided device.

Use of the device must be limited to the individual, and not be shared resources (e.g., a family device).

**Device Security**

***Anti-virus and software security patching:*** The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the individual to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

The school requires that any device used for accessing school systems in the Cloud must have adequate anti-virus software where available. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that are going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

***Password/PIN protection****:* All devices must be secured by a unique password or security pin to ensure that access to the device is limited to named individual permitted to access the school's personal data. Devices that lack the ability to enforce this level of security must not be used for access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. A robust password would provide an additional layer of protection.

***Personal apps:*** Individuals are asked to be mindful of the apps installed on personal devices that they use to access school data. Some of these apps may have enhanced privileges and tracking within them that monitors use of the device and other items that are being accessed. This should be detailed in the app's terms and conditions and the individual should seek assurance that this risk is being managed.

***Equipment disposal:*** When a device being used to access school information is disposed of, it is the responsibility of the individual, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

***Physical security:*** Individuals should ensure any device used to access school data is kept safely secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, transported without sufficient protection to prevent accidental damage etc.

**Email and Internet Activity**

***Use of personal email accounts****:* The School does not permit any individual to use personal email accounts when processing personal data from the school, and therefore information cannot be sent to private email accounts for accessing outside of the school systems.

**System and Accounts Security**

When accessing data held in the Cloud via an internet connection (e.g., Microsoft 365), individuals must ensure that their account is closed when not in use but logging out of the system.

Individuals are responsible for ensuring any internet connection used to access school data must be secured through the use of access controls (a specific user name and password). Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

**Permitted Activity**

Whilst using their own devices, individuals are permitted to access, review and process personal data within the school system with which it is held (e.g., Outlook when responding to an email).

It is not permitted for the data to be downloaded and saved onto any personal device. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within the school's records management system for its full life cycle; including secure destruction in line with the schools retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require individuals to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

**Data Breaches**

In the event of a data breach individuals must follow the process detailed in the Information Security Incident Management Reporting Policy.

### Exemption Process

An exemption to any element of this policy can only be authorised by the school's Senior Information Risk Owner (SIRO). Authorisation will only be given where there is a clear business need, and following a full risk assessment to ensure risks are mitigated. For example, adequate mitigation measures to protect any personal data processed could include a strict requirement for the relevant staff member to delete the data from their device after use and confirm in writing to the SIRO once complete.

### Authorised Access

Access to school's systems using personal devices is only permitted whilst an individual has authorisation to do so. In the event that the individual leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as an information security incident (data breach) and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left the employment of that employer.

### Devices issued to pupils:

1. Where school devices are provided to support learning, it is expected that pupils/students will bring devices to school as required.
2. The school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
3. The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
4. The school will ensure that school devices contain the necessary apps for schoolwork. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll.
5. Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
6. Users must only photograph people with their informed consent. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately.
7. Devices may be used in lessons in accordance with teacher direction.
8. Devices must be returned to the school once the pupil has left unless the student has these have been bought as part of the joint purchase scheme through the bursary scheme.
9. Parents/Carers are responsible for the setting up and use of any home internet connections.
10. Should express their wishes regarding use of digital images on the digital images permission form (Appendix 4).

### School Mobile and landline phones

1 School mobile phones should only be used to contact staff/parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices and under no circumstances should a pupils or parent/carer be given a member of staff personal mobile number.

2 Staff should not be using personal mobile phones school during working hours when in contact with pupils/students

3 Visitors are required not to use their personal phones whilst on site with any pupil's presence due to all mobile phones containing a camera. Visitors will be asked to sign a declaration on arrival in reception. (appendix 5)

4 Pupils are not permitted to use their mobile phones during lesson times

5 School phones should only be used for school business; use of Directory Enquiries or similar services must not be used as each call is costly and numbers can easily be retrieved using a on-line search engine.

### Insurance

If school equipment (or that loaned by the Specialist teaching service to the school) is then loaned to parents to allow the child to continue with schoolwork then we would consider this to be insured under the school policy. Parents should however be advised of the terms and conditions, e.g. lock away when not in use, not to be left in vehicles; please ask parents to fill in a loan form. Parents are required to sign a loan form (appendix 7) before a device can be taken home.

The school insurance covers contents away from site, provided they are being used for curricular purposes- eg a teacher doing lesson plans or reports on laptops etc - this relates to any items on the inventory/asset register. There is currently £150 excess applicable to each claim; staff may be asked to pay this excess where it is felt the fault was due to their negligence. IT equipment left in a vehicle is NOT insured; staff are encouraged to add this to their car insurance.

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

1 When using digital images, staff should, where appropriate, inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
2 Written informed consent from parents or carers will be obtained before photographs of students/ pupils are published on the school website/social media/local press (Appendix 3).
3 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.
4 Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
5 Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
6 Students/pupils must not take, use, share, publish or distribute images of others without their informed consent.
7 Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
8 Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

### Social Media

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

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform, which enables people to directly interact with each other. The school recognises the numerous benefits and opportunities, which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Personal use: The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communication on behalf of the school with an appropriate disclaimer.
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 provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

1. Ensuring that personal information is not published.
2. Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Online Safety BOOST includes unlimited webinar training on this subject: https://boost.swgfl.org.uk/).
3. Clear reporting guidance, including responsibilities, procedures and sanctions.

### <u>School social media accounts</u>

Anyone wishing to create a school account must present a business case to the LMT which covers the following points:

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

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

School accounts must be monitored regularly, including during holidays. Any comments, queries or complaints made through those accounts must be responded to 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 social media account.

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

**Behaviour**

1. The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
2. 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 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.
3. Anonymous posts are discouraged in relation to school activity.
4. If a journalist makes contact about posts made using social media staff must contact the Headteacher and not respond directly.
5. 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 and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate. Users must ensure that their use of social media does not infringe upon relevant data protection laws, copyright or breach confidentiality**.**
6. The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.
7. Only images where the correct informed consent has been sought can be used.
8. If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.

School staff should ensure that:

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

Personal Use:

1. 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, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
2. Post on personal accounts interpreted as racist, sexist or discriminatory in any way or include distasteful of bullying remarks could result in disciplinary action.
3. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
4. Staff are not permitted to accept friend requests from pupils.
5. Staff are strongly advised not to add parents as ‘friends’ into their personal accounts (although it is accepted that staff may know parents outside of their professional capacity).
6. Staff should not discuss work or post pictures or comments of colleague, students or use the school logo or photos on personal accounts.

Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

In addition, the following recommendations are made for staff who have personal social media accounts:

1. To have your privacy settings locked down but remember that nothing is truly private so consider what personal information you share, however nothing on social media is truly private.
2. To keep your eye on your digital tattoo and keep your personal information private and be aware that once images/statements are posted online they can be freely copied and circulated.
3. To share local/useful information and use it as a networking tool and share your achievements.
4. Take control of your images.
5. To know how to report a problem and to report concerns if you feel that you or someone else is subject to abuse by colleagues through use of a social networking site.
6. Not to accept every friend request or be friends with people you don't really know.
7. Not to post anything you wouldn't want your current employer or a prospective employer to see.
8. Not to allow photos on your page that you show you in an unfavourable light.
9. Not to join groups such as 'Its 5am, I'm drunk and face first in a kebab'.
10. Should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
11. Should ensure that their use of social media does not infringe upon relevant data protection laws or breach confidentiality.

**In relation to Social Media Parents/carers must:**

- Not post pictures of pupils, other than their own, on social networking sites where these photographs have been taken at a school event.
- Not to make negative comments about the school, staff or pupils; parents should make complaints through official school channels rather than posting them on social networking sites.

Parents/carers are encouraged to comment or post positive comments about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, they will be referred to the school's complaints procedure.

**Dealing with incidents of online bullying/inappropriate use of social networking sites**

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll. In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- Expose (an individual) to hatred, ridicule or contempt.
- Cause (an individual) to be shunned or avoided.
- Lower (an individual's) standing in the estimation of right-thinking members of society.
- Disparage (an individual in their) business, trade, office or profession." (National Association of Headteachers).

Users in breach of this policy may be subject to but not limited to; disciplinary action, confiscation of equipment, removal of content or referral to external agencies in the event of illegal activity.

Should serious online safety incidents take place, the following external persons/agencies should be informed.

**Unsuitable/inappropriate activities**
Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems and reported to the police. Other activities e.g., cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

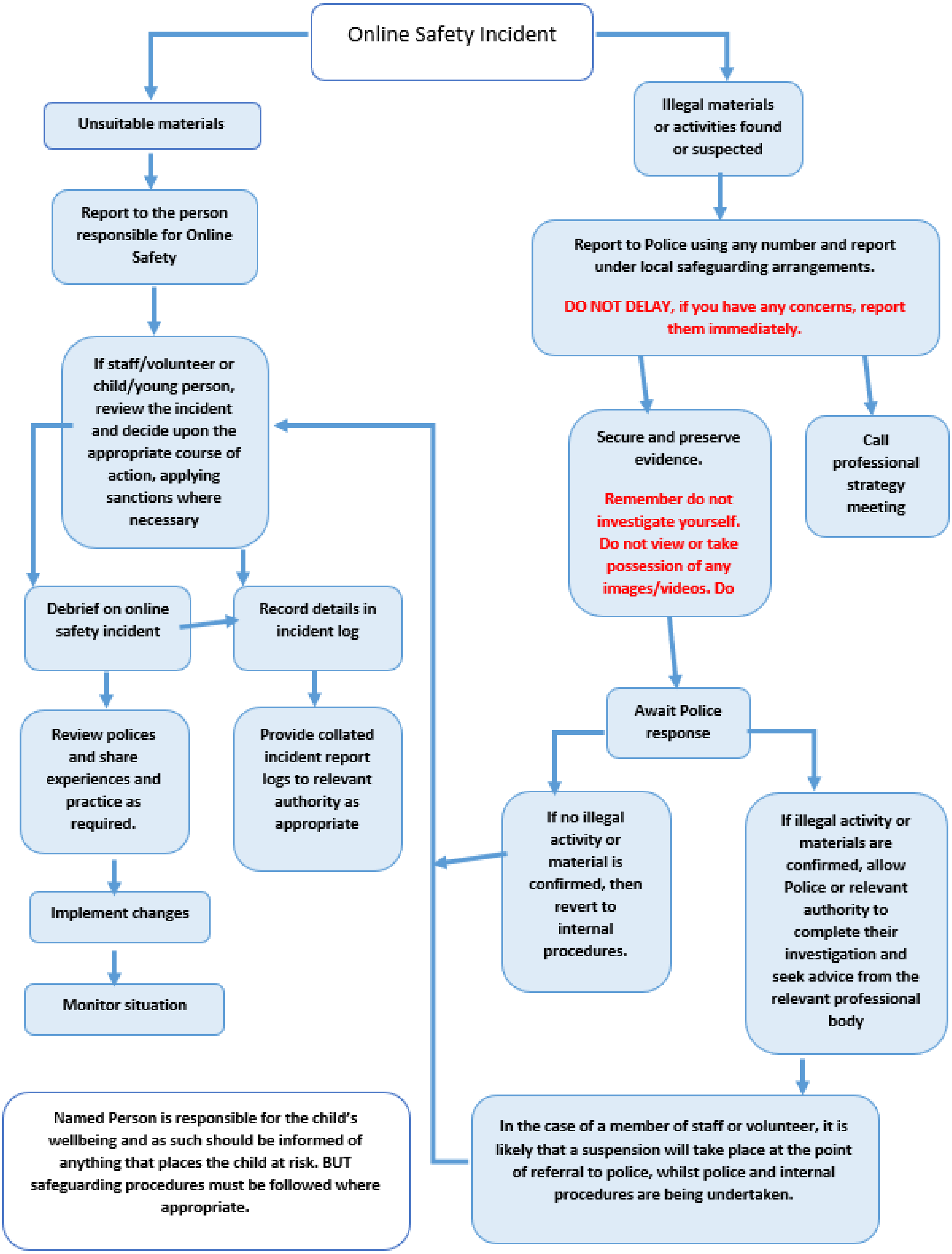
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| Activities that might be classed as cyber-crime that Computer Misuse Act:<br>• Gaining unauthorised access to school networks, data and files through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes or passwords).<br>• Disable/Impair/Disrupt network functionality through the use of computer devices<br>• Using penetration testing equipment (without relevant permission) | | | | | x |
| Using school systems to run a private business | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / | | | | X | |
| Infringing copyright | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | X | | | |
| On-line gaming (non-educational) | | X | | | |
| On-line gambling | | | | X | |
| On-line shopping / commerce | | X | | | |
| File sharing | | | X | | |
| Use of social media | | X | | | |
| Use of messaging apps | | X | | | |
| Use of video broadcasting e.g. Youtube | | X | | | |

### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the *school/academy* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 1 contains a template that can be used in the event of an investigation

### School actions & sanctions

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents are dealt with as soon as possible in a proportionate manner. Incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

## Employee Acceptable Use Policy (AUP)

### Introduction

The AUP applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- Information or data stored on or transferred to removable media
- Information store on portable computing devices including mobile phones, tablets, cameras and laptops
- Speech, voice recordings and verbal communications including voicemail
- Published web content
- Photographs and other digital images

This AUP is intended to ensure that all employees will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

The school will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils and in return expect staff to agree to be responsible users.

### Data

- Have a duty to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) and those emails can be part of the Freedom of Information requests so all correspondence needs to be professional, courteous and respectful. Whilst a copy may have been deleted from the school email, it must be remembered that a copy/ies may still be available by the recipients and as such will still be in existence and is therefore still disclosable by under the GDPR regulations.
- Should only store documents within official school systems and understand that I should not save documents to my desktop as this is not backed up, nor a secure way in which to secure data.
- Should store and delete information/data in accordance with the school's Information Policy.
- Should ensure that any confidential data that is transported from one location to another kept secure; information should never be stored on a USB stick but file access via One Drive or SharePoint should be considered.
- Must be aware that agreements entered by email can form a contract so must only proceed if authorised to do so
- Should log out of equipment when not in use; staff should not use any other member of staff log-ons and should always access equipment under their own username
- Will not access, copy remove or otherwise alter any other user's files, without their express permission
- That any data that I have access to will be kept private and confidential, except when it is deemed necessary by law or by school to disclose such information to an appropriate authority.
- Ensure that when staff take digital images of others, they will do so with their permission and in accordance with the school's policy on the use of digital images. Staff must not use their own equipment to record these images on. Where consent has been given and images are published pupil details will not be used, nor included in any comments.
- Users can only access data to which they have right of access to.
- Access to the server room is restricted and must be kept locked at all times.

**Email/Communications**

The school provided email accounts to employees to assist with performance of their duties. Emails sent from school accounts are the property of the school and as such staff must:

- Be aware that all emails should display the disclaimer message and to contact the Admin staff if they require help in displaying this:

  > *WARNING This email and any attachment to it are confidential. Unless you are the intended recipient, you may not use, copy or disclose either the message or any information contained within the message. If you are not the intended recipient, you should delete this email and notify the sender immediately. Any views or opinions expressed in this email are those of the sender only, unless otherwise stated.*
  >
  > *The Dales School emails and any attachments have not been encrypted; they may therefore be liable to be compromised. Please also note that it is your responsibility to scan emails and any attachments for viruses.*
- If sending confidential or sensitive information by email, ensure it is encrypted or via through the secure email system (currently Egress). The consequence of an e-mail containing sensitive information being sent to the wrong person could incur a civil penalty and be of detriment to the school. If any email is sent to anyone in error a C4C must be completed immediately; it may be necessary for the breach to be reported to the Schools Data Protection Officer in accordance with the School's Information Policy.
- Not open e-mail attachments from an unknown sender; emails from colleagues or known people could also have been cloned, so take care when considering opening any attachment
- Not use emails to carry out my own business or business of others. This includes, but not limited to, work for political organisations, not-for-profit organisations, and private enterprises.
- Never send on chain emails
- Immediately report to a member of LMT, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. (Online Safety BOOST includes an anonymous reporting app Whisper – https://boost.swgfl.org.uk/)
- Ensure that any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Only communicate with pupils and parent/carers using official school systems/emails. Anything required to go on headed paper or use the school logo must be authorised by a member of the leadership team prior to sending.
- All staff must understand that important information is often relayed to staff via email so must ensure that emails sent from LMT are read and if staff are uncertain of the content or meaning should seek clarification.

The school does not permit individuals to send, forward or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

**Internet use**

The school provides internet access to employees to assist with performance of their duties. Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the school
- I understand that school management may have access to their internet browsers and browsing history
- I understand that the school reserves the right to suspend internet access at any time

- I understand that the use of the internet for personal use does not infringe on business functions
- I am aware not to browse or download or send material that could be considered offensive
- I understand that I am not permitted to use the internet to carry out their own business or business of others. This includes, but not limited to, work from political organisations, not-for-profit organisations and private enterprises.
- I understand that I will take care to use the internet in accordance with the school's information Security policy. Users will not click on links on un-trusted or unverified Webpages.
- I am aware that for all technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- I understand that where works is protected by copyright, I will not download or distribute copies (including music and videos)

The school does not permit individuals to use the internet in a way that may be interpreted as insulting, disruptive or offensive by any other individual or entity.

**Social Media Use**

The school recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The school also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people.

The School's Social media account must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the school's information governance policies and data protection legislation.

Staff need to consider the content of their own personal email accounts. Staff should not be social media friends with pupils (including ex pupils). Staff accepting friend's requests from parents, carers is strongly discouraged, however, it is appreciated that these do sometime occur.

**Device Management/security**

In relation to device management all staff should be aware of and comply with the following:

- Only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- Only use passwords for official school log-ons issued to them and not leave them displayed or attached on any equipment.
- Ensure personal passwords are not shared with anyone.
- Be aware that all school devices are controlled though the use of Mobile Device Management software.
- Be aware that all technology issued by the school to individuals, must be handed to a member of leadership team when they leave employment at The Dales School; IT equipment will also be requested to be returned if staff are on long term absence including maternity leave. Failure to do so will incur the school issuing an invoice to that individual for purchase of a new device. New IT will not be issued without prior discussion with a member of LMT.
- To report any accidental access to, or receipt of inappropriate materials, or filtering breach to a member of LMT on a C4C form immediately
- Not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- Not to enter pupil details into any app/website without discussing this first with a member of LMT and completing a data impact statement.
- Ensure anti-virus and other software is kept up to date.
- Ensure any anomalies to the system are immediately reported – early identification and action taken against any virus or malware can prevent loss of data and downtime of the network; in the

event of a Malware attack, do not pay any fines and report to the Action Fraud on 0300 123 2040. Office staff will also follow guidance in appendix 8 to prevent spread.

- Only connect school devices to secure networks.
- Be aware all School IT is subject to routine monitoring by the school; any member of staff must surrender devices upon request.
- Bring issued equipment to school every day, charged and ready for use and be always aware of its whereabouts.
- Keep IT equipment in a secure place when not in use and never leave unattended in a vehicle
- Users are responsible for all parts of equipment issued to them (including chargers) and may be charged for repairs or replacements.
- Report loss, theft or damage immediately to the LMT. If IT equipment requires repair, replacements will not automatically be reissued but will have to wait until an assessment/investigation has been made and a repair conducted. Do not apply permanent marks, decorations or modifications to their issued equipment.
- Food and drink should be kept away from IT equipment
- Admin equipment should be used for the purpose provided and not share this equipment nor should they allow pupils to access their admin iPads
- Must not remove equipment from protective pads, screens or cases – if staff are experiencing a problem with their equipment, they should discuss this with the admin staff
- Never put anything heavy on top of an I-Pad/tablet and ensue that it is always put in a safe and secure place when not in use.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- Staff should not modify the settings of their iPads in any way unless instructed by admin or LMT
- Discuss iTunes/app downloads with the admin staff
- Should not link personal devices to school iPads/Tablets/IT equipment
- Should not subject iPads to extreme temperatures

Understand that if they use their mobile device in school, that they will follow the rules set out in this policy, in the same sway as if I was using school equipment. They will also follow any additional rules set out in this policy about such use.

The Dales School is committed to its mission to continuously innovate and improve processes and systems in order to improve outcomes for the people we support, work in a safe and secure manner and to ensure we play our part when it comes to the sustainability of the Environment. Our vision is to further innovate new systems which would improve service delivery and integrate the best technologies with human expertise.

We save resources and energy by avoiding printing and the associated postage overheads, we ask all others who deal with us to interact with us in this manner where possible.

On the rare occasions where letters do need to be sent to us, once processed, any paper is securely destroyed or carefully recycled.

*The following statement will be added to all staff PRD and must be signed by all staff in accepting of the IT policy*:

I confirm that I have read and understood the School's ICT policy and will comply with all elements within it and agree to use the school digital technology systems within these guidelines.
I understand that this acceptable use policy applies not only to my work and use of school digital equipment in school, but also applies to my use of school systems and equipment off the premises and use of personal equipment on the premises or in situation related to my employment by the school.

I understand that if I fail to comply with this policy, I could be subject to disciplinary action.

Staff Name:

Date:

**Student / Pupil Acceptable Use Agreement Form**
This form relates to the student Acceptable Use Agreement.

- I will ask a teacher or suitable adult if I want to sue the computer/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use the computer/tablet.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).
- I will not take or distribute images of anyone without their permission.
- I will act as I expect others to act toward me
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

The school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students/pupils to agree to be responsible users.

.

Appendix 1:

# Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: ………………………………………………………………………………

Date: ………………………………………………………………………………

Reason for investigation: ……………………………………………………………………………………………

……………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………

Details of first reviewing person

Name: ……………………………………………………

Position: ……………………………………………………

Signature: ……………………………………………………

Details of second reviewing person

Name: ……………………………………………………

Position: ……………………………………………………

Signature: ……………………………………………………

Name and location of computer used for review (for web sites)

……………………………………………………………………………………………………………………………

…………………………………………………………………………………………………

| Web site(s) address/device | Reason for concern |
|---|---|
| | |
| | |
| | |

Conclusion and Action proposed or taken

| | |
|---|---|
| | |
| | |
| | |

**Appendix 2:** Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. The school also operates a physical monitoring approach where staff working directly with pupils using technology will closely supervise pupils them.

The responsibility for the management of the school's filtering policy will be held by Coorecom and LMT. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- Be logged in change control logs.
- Be reported to a second responsible person (Headteacher/SBM)
- Be reported to and authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to a member of the leadership team any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

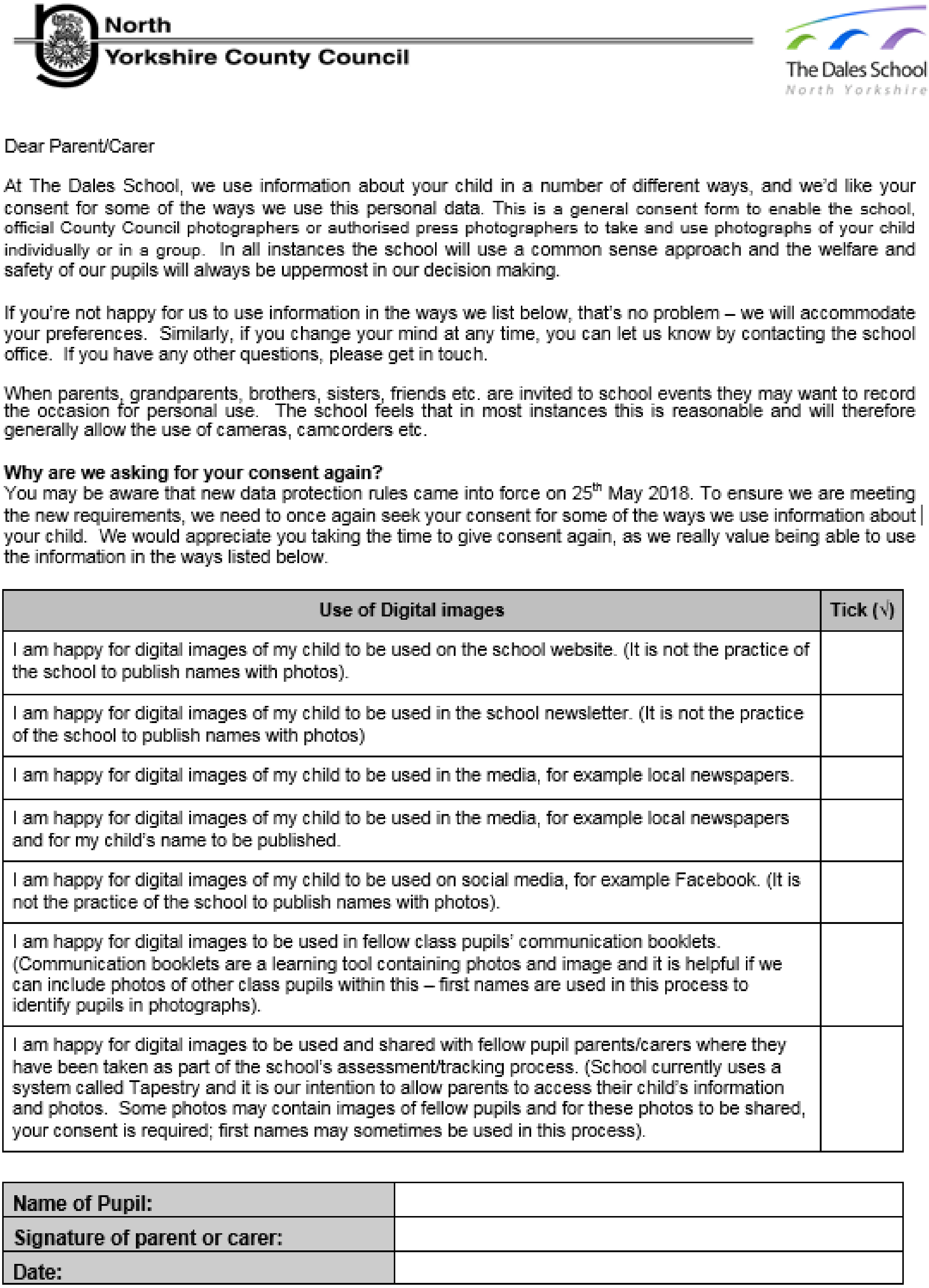
Differentiated internet access is available for staff and customised filtering changes are managed by the school. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by Coorecom as part of the Wi-fi service.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or member of LMT.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to LMT.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded.
- Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to LMT will decide whether to make school level changes (as above).

**Education/Training/Awareness:** Anyone accessing the internet will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

**Audit / Reporting:** Logs of filtering change controls and of filtering incidents will be made available to LMT

## Appendix 3: Photo consent



North Yorkshire County Council

The Dales School
North Yorkshire

Dear Parent/Carer

At The Dales School, we use information about your child in a number of different ways, and we'd like your consent for some of the ways we use this personal data. This is a general consent form to enable the school, official County Council photographers or authorised press photographers to take and use photographs of your child individually or in a group. In all instances the school will use a common sense approach and the welfare and safety of our pupils will always be uppermost in our decision making.

If you're not happy for us to use information in the ways we list below, that's no problem – we will accommodate your preferences. Similarly, if you change your mind at any time, you can let us know by contacting the school office. If you have any other questions, please get in touch.

When parents, grandparents, brothers, sisters, friends etc. are invited to school events they may want to record the occasion for personal use. The school feels that in most instances this is reasonable and will therefore generally allow the use of cameras, camcorders etc.

**Why are we asking for your consent again?**
You may be aware that new data protection rules came into force on 25th May 2018. To ensure we are meeting the new requirements, we need to once again seek your consent for some of the ways we use information about your child. We would appreciate you taking the time to give consent again, as we really value being able to use the information in the ways listed below.

| Use of Digital images | Tick (√) |
|---|---|
| I am happy for digital images of my child to be used on the school website. (It is not the practice of the school to publish names with photos). | |
| I am happy for digital images of my child to be used in the school newsletter. (It is not the practice of the school to publish names with photos) | |
| I am happy for digital images of my child to be used in the media, for example local newspapers. | |
| I am happy for digital images of my child to be used in the media, for example local newspapers and for my child's name to be published. | |
| I am happy for digital images of my child to be used on social media, for example Facebook. (It is not the practice of the school to publish names with photos). | |
| I am happy for digital images to be used in fellow class pupils' communication booklets. (Communication booklets are a learning tool containing photos and image and it is helpful if we can include photos of other class pupils within this – first names are used in this process to identify pupils in photographs). | |
| I am happy for digital images to be used and shared with fellow pupil parents/carers where they have been taken as part of the school's assessment/tracking process. (School currently uses a system called Tapestry and it is our intention to allow parents to access their child's information and photos. Some photos may contain images of fellow pupils and for these photos to be shared, your consent is required; first names may sometimes be used in this process). | |

| | |
|---|---|
| **Name of Pupil:** | |
| **Signature of parent or carer:** | |
| **Date:** | |

Appendix 4: Digital consent for communication device letter

Dear Parent/Carer

**Communication Book**

Your son/daughter is to be issued a communication book they can use both in school and at home. This contains digital images of your child/young person as well as other pupils from the Dales School for which we have parental consent to use. Please be aware that parents/carers have the right to withdraw this consent and if this happens, we will need to remove these images.

In addition, as these images are classed as personal data, we need to ensure that they are used only for the purpose for which consent is given and ask that you complete and sign the declaration below before the book can be issued.

______________________________________________________________________

**Communication Book Declaration**

I confirm that I will not copy, share or reproduce the images of staff or pupils contained in my child/young person's communication book.

I also confirm that I will endeavour to keep this book safe and immediately report any loss of this book.

Pupil name ____________________________________________________________

Parent/Carer name: ______________________________________________________

Parent/carer signature: ____________________________________________________

Date: ________________

*For school admin use*

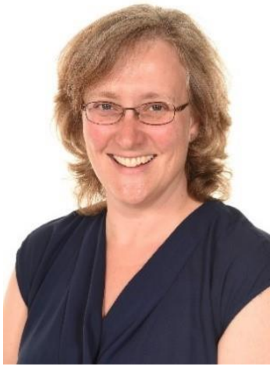
*Date book issued:*
*Names of pupils contained within this book:*

Appendix 5: Community Users letter

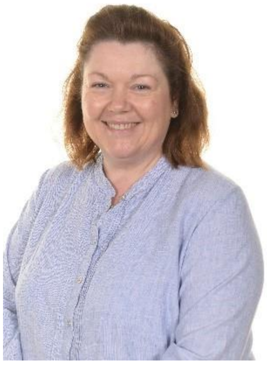
Dear Visitor

**Safeguarding information**
As a welcome visitor to our school today, it is imperative that you follow our safeguarding policy. Prior to your entry into school, please sign overleaf to indicate your commitment to the safety and welfare of all the children and young people in our school community.

**Safeguarding Leads**
If you see anything that causes you concern regarding the safety and/or welfare of a child/young person/staff member whilst in school today, this must be reported to a Designated Safeguarding Lead (pictures and names shown below). Office staff will be able help you locate these staff if necessary.



Ann-Marie Ellis
Headteacher



Sharon Kettleborough
Deputy Headteacher

**Mobile Phone Policy**
As part of our ongoing commitment to uphold the very best safeguarding practice for all of our pupils, staff, partners and visitors, I wish to make explicitly clear the non-negotiables for use of mobile phones when on site at The Dales School. By signing the form, you are agreeing:

- To keep your phone in your locker or bag whilst you are class based or working with pupils.
- Not to use your mobile phone whilst working with/supporting a pupil
- Not to use your mobile phone in any areas where other pupils are present, even if you are not working directly with them
- Not to take pictures of our children or young people

You are very welcome to hand your phone into reception and we will keep it locked in a safe place until your departure.

If the purpose of your visit requires the use of a mobile phone for any reason, you are advised to discuss this with a Designated Safeguarding Lead.

**Lanyard and further information**
Further information is also available in your lanyard and more detail can be provided on request.

**Acceptable Use Agreement**
**This Acceptable Use Agreement is intended to ensure:**

- That community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of these systems and devices.

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user’s files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment 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 understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

By signing the form, you are agreeing that you have read and understand your commitment to supporting the school with its safeguarding practices as detailed in this letter.

Name:

Signed: ____________Date:

*As the school is collecting personal data by issuing this form, we are informing you that school staff will have access to this information; that it will be stored securely in the school office and retained for 3 years following your last visit after which time it will be destroyed.*

Appendix 6: **Employee equipment issue form**

**Name: …………………………………………………………………………………………………**

I acknowledge that I have received the following equipment to enable me to complete admin tasks associated with my role.

| | Issued to: | Make/Model | Serial number | Charger issued | Asset tag number |
|---|---|---|---|---|---|
| Laptop | Middle leaders | | | | |
| Ipad | Middle leaders & ATA & Acting ATA | | | | |
| Fire Pads | GTA & PSA | | | | |

- I understand that it is my complete responsibility to keep equipment in a safe place at all times.
- I am aware that if the equipment is broken, stolen or damaged; it is my responsibility to immediately report this to a member of LMT. I also understand that I may be charged for any damages that occurred while in my possession that are a result of misuse or carelessness, including loss/replacement of chargers.
- I understand that once my employment ends, it is my responsibility to return all equipment signed out to me. In addition, devices also need to be returned to school during a long absence such as sickness, maternity or secondments.
- I understand that I am required to submit device(s) for audit/PAT testing on request
- I understand that I must not remove any device from protective sleeves/cases
- I understand that I must not change any pin numbers issued to me.
- I understand that I must not leave anything on the device with passwords/pins numbers written on
- I understand that it is my responsibility to the device up to date and check for updates on systems and apps.
- I understand that these are admin devices and issued personally to each member of staff; devices should not be given to pupils to use.
- I confirm that I have read the ICT policy and updated my PRD confirming this and compliance with this Policy

**Additional important information re use of Fire Pads**

- All Firepads share an account, therefore no additional apps can be downloaded to these devices without discussing this first with a member of LMT (any app downloaded will then appear on all the other devices)
- Photos must not be stored on the device, but immediately either uploaded into Tapestry or onto your personal school Onedrive account.

Signed:

Dated:

## Appendix 7: Equipment loan letter

Dear

Your son/daughter ___________ has been given an _______________communication app. This is on loan from The Dales School to support _____________________ to develop their communication, therefore no other app can be downloaded onto the device.

While _____________ remains at The Dales School, the communication aid is insured through North Yorkshire County Council. If the device is damaged while at home you will be asked to contribute towards the device being repaired or replaced. This currently stands at £150.

The communication aid must be returned when:

1. It is no longer required

2. It is replaced by an updated communication aid

3. Leavers the Dales School

Please sign the agreement form below and return to school.

Yours sincerely

-----------------------------------------------------------------------------------------------------------

I am in receipt of an: ………………………………… communication aid for the use of my son/daughter. I understand that the device is on loan from The Dales School. I agree that if the device is damaged while at home I will contribute towards the repair or replacement.

Name of pupil:

Name of parent/carer:

Signature of parent/carer:

Date:

**Appendix 8:** Ransomware

Ransomware, or ‘crypto malware’ is a form of malicious software that is used to hold computers and data to ransom until a payment is made. When hit a computer will generally display a message explaining that everything has been encrypted and a message on how to make payment. Depending on attack, files may become inaccessible immediately and everything accessible from your computer will be encrypted.

**How to protect yourself from a Malware attack**

- Don’t click on links, or open any attachments if you receive unsolicited emails or SMS messages. The links may lead to malicious websites and any attachments could be infected with malware.
- Always install software updates as soon as they’re available. Whether you’re updating the operating system or an application, the update will often include fixes for critical security vulnerabilities
- Install anti-virus software on your computer and mobile devices and keep it updated.
- Websites can trigger pop-up messages claiming that your computer is infected or needs updating. Clicking on these pop-ups would activate the download of the ransomware and infect your computer. Ransomware can often be picked up from visiting disreputable sites including illegal movie streaming websites and some adult sites
- Memory sticks being transferred between different computers can assist in the spreading of infection and as such are not allowed to be connected to school computers.
- Create regular backups of your important files.
- To ensure updates can take place, please ensure ALL computers are shut down at the end of each day.

**If you think you may be a victim:**

1. Turn off your computer immediately
2. Unplug the network cable
3. Report it to LMT IMMEDIATELY
4. Write down what you have done as finding the source may help speed up recovery

In addition:

- Report to Action Fraud on 0300 123 2040
- Don’t pay extortion demands as this only feed into criminals’ hands and there’s no guarantee that access to your files will be restored if you do pay.