Boroughbridge Primary School and Nursery

Online and E-Safety Policy

Date Adopted	Date for Review	Person/s Responsible
March 2024	March 2025	Deputy Headteacher
Approved by:	Emma Ryan Headteacher	Tim Collin Governor

This Policy is valid from the date as recorded, thereby invalidating any other preceding policy.

Where a 'named' person is no longer in post, this policy remains valid until the next review date.

Contents

1. Introduction

This online safety policy recognises the commitment of our school to keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It is in place due to the requirements set out in the following government documents:

- Keeping children Safe in Education 2022
- Teaching online safety in Schools 2019

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (E.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.

(DfE Keeping Children Safe in Education 2022)

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise, and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

The scope of this policy

- This policy applies to the whole school community including the Senior Leadership Team (SLT), Governing Body (GB), all staff employed directly or indirectly by the school, visitors, and all pupils.
- The Senior Leadership Team and school governors will ensure that any relevant or new legislation that may impact upon the provision for online safety within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of 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 online bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online behaviour that take place out of school.

Implementation of the policy

- The Senior Leadership Team will ensure all members of school staff are aware of the contents of the school Online Safety Policy and the use of any recent technology within school.
- All staff, pupils, occasional and external users of our school ICT equipment will sign the relevant Acceptable Use Agreements.
- All amendments will be published, and awareness sessions will be held for all members of the school community.
- Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- The Online Safety Policy will be made available to parents, carers, and others via the school website.

2. Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community and that everyone has their part to play in ensuring all members of the community can benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The senior leadership team

- The headteacher and governing body will take ultimate responsibility for the online safety of the school community
- The Headteacher, Mrs. Emma Ryan has the role of designated safeguarding lead (DSL) to take lead responsibility for safeguarding and child protection (including online safety) Mr Neil Ryder supports her as the deputy designated safeguarding lead who can take responsibility for safeguarding and child protection (including online safety) in her absence.
- Mr Neil Ryder is designated as the online safety lead who takes on day to day responsibility for online safety; provide staff with training; monitoring the effectiveness of this policy and can support any of our community in this area.
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the governors
- Develop and promote an online safety culture within the school community
- Ensure that all staff, pupils, and other users agree to the Acceptable Use Agreement and that new staff have online safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they can carry out their roles effectively regarding online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

Employees and Visitors

- Read, understand, and help promote the school's online safety policies and guidance
- Read, understand, and adhere to the employee and visitors acceptable use agreement
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current online safety issues, legislation, and guidance relevant to their work
- Always maintain a professional level of conduct in their personal use of technology
- Ensure that all digital communication with pupils is on a professional level and only through school-based systems, **NEVER** through personal email, text, mobile phone, social network, or other online medium
- Embed online safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and/or to their line manager
- Respect, and share with pupils the feelings, rights, values, and intellectual property of others in their use of technology in school and at home

Technical Staff

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps, including filtering and monitoring, are in place to safeguard the security of the school IT system, sensitive data, and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and detection and prevention of malicious attack
- At the request of the Leadership Team conduct periodic checks on files, folders, email, internet use and other digital content to ensure that the Acceptable Use Agreement is being followed
- Report any online safety related issues that come to their attention to the DSL, online safety lead and/or senior leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the local authority, internet providers and others as necessary on online safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Pupils

- Read, understand, and adhere to the pupil Acceptable Use Agreement and follow all safe practice guidance
- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values, and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening

- Report all online safety incidents to appropriate members of staff
- Discuss online safety issues with family and friends in an open and honest way
- To know, understand and follow school policies on the use of mobile phones, digital cameras, and handheld devices
- To know, understand and follow school policies regarding online bullying

Parents and Carers

- Help and support the school in promoting online safety
- Read, understand, and promote the pupil Acceptable Use Agreement with their children
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology
- To give/or not consent for the school to use electronic images of their child internally and to publish them online.
- Adhere to the Parent, carer, and visitor behaviour policy.

Governing Body

- Ensure there is a whole school approach to online safety which is reflected in relevant policies, the school curriculum, teacher training, the DSL role and parental engagement
- Read, understand, contribute to, and promote the school's online safety policies and guidance as part of the school's overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the school IT infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for the school to implement the online safety strategy
- Ensure the school has appropriate filters and monitoring systems in place and regularly review their effectiveness.

Visitors

- Take responsibility for liaising with the school on appropriate use of the school's IT equipment and internet, including providing an appropriate level of supervision where required
- Ensure that participants follow agreed Acceptable Use Agreements

3. Acceptable Use Agreements (AUA)

School has a number of Acceptable Use Agreements for different groups of users.
These are shared with all users yearly. Pupils, employees, and visitors will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to school who use our ICT facilities are made aware of the appropriate agreements.

4. Training

Technology use changes at a fast pace, and we recognise the importance of regular staff training. All newly appointed staff will have online safety training at induction. The online safety lead will attend regular training updates as necessary, and keep up to date through online resources, newsletters, and networks. All school staff will receive termly updates on risks to pupils online from the online safety bulletin and attend training, as necessary.

5. Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Online safety is taught in specific Computing and PSHE/RSHE lessons and embedded across the curriculum, with pupils being given regular opportunities to apply their skills.

We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.
We discuss, remind, or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the Acceptable Use Agreements.
Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

6. Remote education and home learning

In response to emergency closures or a child needing to be educated offsite the school uses the following online learning resources: Microsoft Teams, Google Workspace, Purple Mash, Parent Email.

These will be used as necessary in circumstances where a child or group of children must quarantine or self-isolate, or when the school needs to close in an emergency for any reason.

All Acceptable Use Policies will apply to school resources which are accessed in the home environment. Parents and carers will be informed of the online resources pupils are expected to access, and which staff pupils will communicate with online.
The following DfE guidance will be used:
https://www.gov.uk/guidance/safeguarding-and-remote-education DfE March 2021

7. How parents and carers will be involved

We believe it is important to help all our parents and carers develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will offer opportunities for finding out more information through the school newsletter and website.

We will ask all parents to discuss the pupil's Acceptable Use Agreements with their child and return a signed copy to the school. We also ask parents to sign the home school agreement which includes a statement about their use of social networks in situations where it could reflect on our school's reputation and on individuals within the school community.

We request our parents to support the school in applying the Online Safety Policy.

8. Managing and Safeguarding IT systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up to date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. head teacher and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by the technician after agreement with the Senior Leadership Team.

We do not allow anyone except technical staff to download and install software onto the network. Staff are allowed administrator rights to download software on school provided laptops.

Filtering

To be compliant with the Prevent Duty and Safeguarding Children in Education 2016, the school will:

- As part of the Prevent duty, conduct an annual assessment of the risk to pupils of exposure to extremist content in school
- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by North Yorkshire County Council. They block access to illegal child abuse images and content. They filter the police assessed list of unlawful terrorist content produced on behalf of the home office. The school is satisfied that web filtering manages most inappropriate content including extremism, discrimination, substance abuse, pornography, piracy, copyright theft, self-harm, and violence. However, it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.
- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the Acceptable Use Agreement and appropriate sanctions taken.
- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.
- Post notices in classrooms and around school as a reminder of how to seek help.

Monitoring

To be compliant with the current Prevent Duty and Keeping Children Safe in Education, the school will:

- Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.
- Pupils are always supervised by staff while using the internet as this reduces the risk of exposure to extremist, illegal or inappropriate material; direct supervision also enables school staff to take swift action should such material be accessed either accidentally or deliberately.
- Internet and network use is monitored regularly by the school technician to identify access to websites or internet searches which are a cause for concern.

- Network monitoring software is used throughout school. This produces reports of inappropriate communications, searches, and website access. The reports are checked regularly by the IT Technician/Network Manager and any cause for concern is reported to the Senior Leadership Team.

Access to school systems
The school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private, or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third-party users.

Passwords
- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually named user account and password for access to IT equipment, email, and information systems available within school.
- Children have access to online accounts which have individual log-in details for Collins e-library (YR-Y2), Times tables rock stars (Y2 – Y6), Google workspace, Microsoft Teams, Purple Mash, Numbots (YR – Y1).
- Children have access to a variety of devices that connect though our wireless network. These include Windows laptops, Google Chromebooks, Android tablets and iPad. These devices are only accessible with access codes and usernames. When using these devices, the children are supervised by adults.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains a log of all accesses by users and of their activities while using the system to track any online safety incidents.

9. Using the internet
We provide the internet to
- Support teaching, learning and curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards, and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity

can be monitored and checked.

All users of the school IT or electronic equipment will always abide by the relevant Acceptable Use Agreement, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an email account for school-based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. Email messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school email system is monitored and checked.

It is the personal responsibility of the email account holder to keep their password secure.
As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

School will set clear guidelines about when pupil-staff communication via email is acceptable, and staff will set clear boundaries for pupils on the out-of-school times when emails may be answered.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email address.

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

Publishing content online

School website

The school maintains editorial responsibility for any school-initiated web site or publishing online to ensure that the content is accurate, and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, email, and telephone number. Contact details for staff published are school provided.

Identities of pupils are always protected. Photographs of identifiable individual pupils are not published on the website and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents, or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Pupils will only be allowed to post or create content on sites where members of the public have

access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school
Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video, and sound
We recognise that many aspects of the curriculum can be enhanced using multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using, and storing digital images, video, and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the filename or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and on the website.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera, or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own, they should not be uploaded to social media sites.

Using video conferencing, web cameras and online meeting apps

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls, or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought

if the material is to be published.

For their own protection, a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the headteacher or line manager and respective parents and carers.

Using mobile phones

Pupils

Personal mobile devices belonging to Year 6 pupils are permitted but must not be used on school premises. They must be turned off as the child enters the school site then handed in to a member of staff when entering the building. They must be collected from a member of staff at the end of the school day and not switched on until the child has left the school site. Personal devices are brought onto school premises by pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

Staff

Staff are not permitted to use their personal ICT equipment in school. However they can use personally owned mobile phones. Mobile phones will never be used to take photos of children for example at events in school or out of school (e.g. sporting events). Staff bringing mobile phones into school must ensure there is no inappropriate or illegal content on the device. Phones should be switched off or on silent when children are present. Devices connected to mobile phones such as smart watches, should also be set to silent and notifications disabled. Phones can be used at break and lunch times but should never be used where children are present.

In very exceptional circumstances, such as a family emergency, staff should seek permission from the Headteacher to use their mobile devices during working hours. This should happen away from children. The schools main telephone number can be used for emergencies by staff or volunteers or by people who need to contact them. Where undertaking off-site activities and if there is an emergency that requires it, a teacher may use their mobile phone to contact school or the emergency services. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a parent. In an emergency, where a staff member needs to contact a parent with their personal device, they should hide (by inputting 141) their own mobile number for confidentiality purposes.

Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request. If the victim is another pupil or staff member, we do not consider it a defence that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress is online bullying; this will be considered a disciplinary matter.

We make it clear to staff, pupils, and parents that the Headteacher has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Adult visitors on site

We recognise that visitors and governors may wish to have their personal mobile devices with them for use in case of emergency. However, safeguarding the children within the school is

paramount and it is recognised that personal mobile devices have the potential to be used inappropriately.

Mobile devices should never be used in the presence of children when in the school grounds or building.

Personal devices cannot be used to take photos of pupils

Using wearable technology
Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school premises however as there is no internet service to use in school and children's mobiles phones are switched off as they arrive on site, the functions on these devices are limited. Any wearable devices must only be used for step and fitness tracking when in school. Any devices that record audio or visual must not be used in school. Personal devices are brought onto school premises by pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Wearable tech for additional needs.

Some children and adults use wearable technology for medical or additional needs. These devices must be used in accordance with the policy where applicable and any use outside of the policy must be agreed with the headteacher.

10. Protecting school data and information
School recognises the obligation to safeguard staff and pupils' sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the General Data Protection Regulations (GDPR) 2018 and we always comply with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with secure cloud storage for storing all data
- Portable devices which store information such as memory sticks or cameras must not be used to transport information between school and home.
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the school management information system holding pupil data. Passwords are not shared, and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school

- All devices taken off site, e.g. laptops, tablets, removable media, or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them
- Remote access to computers is by authorized personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example governors, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

Management of assets
Details of all school-owned hardware and software are recorded in an inventory.

The inventory is checked annually to ensure data and information is secure. All redundant IT equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013.

11. Responding to online safety incidents
All online safety incidents are recorded and logged on CPOMs which is regularly reviewed.
Any incidents where pupils do not follow the Acceptable Use Agreement will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the DSL, who will then respond in the most appropriate manner.

Instances of online bullying will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's online safety lead and technical support and appropriate advice sought, and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures, or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology
If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer, then all Safeguarding Procedures and Guidance will be followed.

Dealing with complaints and breaches of conduct by pupils
- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to the DSL and a senior member of staff

- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal)

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, in breach of the Equalities Act or violent/threatening violence
- online peer on peer abuse and sexual harassment
- continuing to send or post material regarded as harassment or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, which is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos, and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 2018

12. Reviewing online safety

An annual review of online safety policy and practice will be conducted.