Online Safety

2025 - 2026

‘Because Children Deserve Better’

Reviewed By:	Tina Quirke, Lead Social Worker and DSL
Approved By:	Kathryn Parkinson, Chief Operating Officer
Responsible Person:	Tina Quirke, Lead Social Worker and DSL
Policy Number:	6:8 V2
Date:	August 2025
Next Review Date:	August 2026

Contents

1. Introduction

This online safety policy recognises the commitment from Pivot to keeping staff and learners safe online and acknowledges its part in Pivot's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep learners safe when using technology. 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 frauds. If you feel your learners, students or staff are at risk, please report it to your DSL (Designated Safeguarding Leads) who will report it to the Anti-Phishing Working Group.

(DfE Keeping Children Safe in Education 2025)

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 Pivot 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 learners.

Our expectations for responsible and appropriate conduct are set out in our ICT Acceptable Use Policy (AUP) which we expect all staff and learners 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 Pivot community including staff and learners.

The directors, lead social worker and site senior leadership teams 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 headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the Pivot 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 outside of a Pivot setting, but is linked to membership of Pivot.

The Education Act 2011 gives Pivot 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.

Pivot 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 outside of Pivot.

The person(s) in school taking on the role of Designated Safeguarding Lead (DSL) are:

Name	**Site**
Amy Lawrence	Leeds Links and Elevate
Jean Chamley	Leeds Core Offer
Emma Jane Barber	Kirklees Lower
Emma Goddard	Kirklees Upper
Amy Thornton	Kirklees Pivot Outreach Programme
Rebecca Hall	Wakefield Pivot Outreach Programme
Tom Laurie	Pivot 6

At each setting, the deputy headteacher is the nominated online safety lead.

Implementation of the policy

The senior leadership team will ensure all members of school staff are aware of the contents of the Online Safety Policy and the use of any modern technology within Pivot settings.

All staff, learners, occasional and external users of our ICT (Information and Communications Technology) equipment will sign the relevant Acceptable Use Policy.

All amendments will be published, and awareness sessions will be held for all members of the Pivot community.

Online safety will be taught as part of the curriculum in an age-appropriate way to all learners.

Online safety posters will be prominently displayed around Pivot settings

The Online Safety Policy will be made available to parents, carers and others via the Pivot website or other online learning tools/apps.

The following national guidance are acknowledged and included as part of our Online Safety Policy:

Government Guidance

Keeping Children Safe in Education (DfE 2025)

Teaching Online Safety in School (DfE 2019)

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2015)

How social media is used to encourage travel to Syria and Iraq - Briefing note for schools (DfE 2015)

Cyberbullying: Advice for Headteachers and School Staff (DfE 2014)

Sharing nudes and semi-nudes: advice for education settings working with children and young people (DfE 2020)

Sexual violence and sexual harassment between children in schools and colleges (DfE 2021)

Kirklees Learning Service Guidance

The following Kirklees guidance documents are included as part of this Online Safety Policy:
Kirklees Electronic Communications Guidance for School Staff

Leeds Safeguarding Children's Partnership
https://www.leedsscp.org.uk/practitioners/guidance/e-safety

Other Guidance

Appropriate Filtering for Education Settings (UK Safer Internet Centre)

Appropriate Monitoring for Schools (UK Safer Internet Centre)

2. Responsibilities of the Pivot community

We believe that online safety is the responsibility of the whole Pivot 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 accepts the following responsibilities:

- The directors and headteachers will take ultimate responsibility for the online safety of the Pivot community
- Appoint a senior member of staff to the role of designated safeguarding lead (DSL) to take lead responsibility for safeguarding and child protection (including online safety)
- The school's deputy headteacher is the online safety lead
- 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 Pivot's information and data assets
- Ensure liaison with the directors
- Develop and promote an online safety culture within the Pivot community
- Ensure that all staff, learners, and other users agree to the Acceptable Use Policy 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 Pivot 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 at Pivot and review incidents to see if further action is required

Responsibilities of the DSL:

- Be the first point of contact in the setting on all online safety matters
- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, online bullying, radicalisation, and others.
- Attend regular training and updates on online safety issues. Stay up to date through use of online communities, social media, and relevant websites/newsletters.
- Ensure delivery of an appropriate level of training in online safety issues
- Ensure that staff and learners know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident
- Liaise with the Local Authority, the Local Safeguarding Children's Partnership, and other relevant agencies as appropriate
- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.
- Raise awareness of the issues which may arise for vulnerable learners in the school's approach to online safety ensuring that staff know the correct child protection procedures to follow.

Responsibilities of the online safety lead:

- Promote an awareness and commitment to online safety throughout the setting
- Take day to day responsibility for online safety within the setting working with the DSL
- Develop an understanding of current online safety issues, guidance, and appropriate legislation through regular training
- Ensure that online safety education is embedded across the curriculum
- Ensure that online safety is promoted to parents and carers
- Ensure online safety concerns are logged on CPOMS to accurately record and reflect incidents
- Ensure that good practice guides for online safety are displayed in classrooms and around the setting
- To promote the positive use of technologies and the internet

Responsibilities of all staff:

- Read, understand, and help promote Pivot's online safety policies and guidance
- Read, understand, and adhere to the staff AUP
- 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 learners 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 learners at all times when engaged in learning activities involving technology

- Ensure that learners 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 CPOMS/Arbor and/or to their line manager
- Respect, and share with learners the feelings, rights, values, and intellectual property of others in their use of technology in school and at home

Additional responsibilities of lead social worker/ DSL technical support and business managers:

- Support Pivot in providing a safe technical infrastructure to support teaching and learning
- Ensure appropriate technical steps, including filtering and monitoring, are in place to safeguard the security of the Pivot IT system, sensitive data, and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse, 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 Policy is being followed. The checks undertaken are detailed in the quality assurance cycle which is updated each year.
- 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

Responsibilities of learners:

- Read, understand, and adhere to the learner AUP 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 Pivot
- Ensure they respect the feelings, rights, values, and intellectual property of others in their use of technology at Pivot 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 Pivot's policies regarding online bullying

Responsibilities of parents and carers:

- Help and support Pivot in promoting online safety
- Read, understand, and promote the learner AUP 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 Pivot if they have any concerns about their child's use of technology
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images of learners
- To agree to and sign the home-school agreement containing a statement regarding their personal use of social networks in relation the school:

We will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Responsibilities of the directors

- 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 Pivot's online safety policies and guidance as part of the Pivot overarching safeguarding procedures
- Support the work of each setting in promoting and ensuring safe and responsible use of technology in and out of Pivot, including encouraging parents to become engaged in online safety awareness
- To have an overview of how the Pivot IT infrastructure provides safe access to the internet and the steps Pivot takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for Pivot to implement the online safety strategy
- Ensure Pivot has appropriate filters and monitoring systems in place and regularly review their effectiveness

3. Acceptable use policy

Pivot have an acceptable use policy. This is shared with all users yearly and staff and learners will be expected to agree to them and follow the guidelines. We will ensure that external groups and visitors to Pivot who use our ICT facilities are made aware of the Pivot ICT and Internet Acceptable Use Policy 2025-26.

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 DSL's and online safety lead will attend regular training updates as necessary, and keep up to date through online resources, newsletters, and networks. All Pivot staff will receive regular updates at least annually on risks to learners online from the DSL's and online safety lead and attend online or external training, as necessary.

5. Learning and teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our Pivot community lies in effective education. We know that the internet and other technologies are embedded in our learners' lives, not just in Pivot settings but outside as well, and we believe we have a duty to help prepare our learners 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 learners 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 learners being given regular opportunities to apply their skills.

We teach learners how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and learners 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 learners 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 learners about the responsibilities to which they have agreed through the Acceptable Use Policy.

Learners 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 learner needing to be educated off-site Pivot uses the following online learning resources:

Teams, Google Classroom, TT Rock Starts, Class DoJo, BKSB, Century Learning, Academy 21, learner/parent email.

These will be used as necessary in circumstances where a child or group of children are educated off site or must quarantine or self-isolate, or when the setting needs to close in an emergency for any reason. Acceptable Use Policy will apply to school resources which are accessed in the home environment. Parents and carers will be informed of the online resource's learners are expected to access and which staff learners 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 meetings, the school newsletter and website.

We will ask all parents to discuss the AUP with their child and sign the Pivot data collection pack to confirm agreement. 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 Pivot's reputation and on individuals within the Pivot community.

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

8. Managing and safeguarding IT systems

Pivot will ensure that access to the 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 Pivot activity.

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

The wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access once inducted via the school's business managers.

We do not allow anyone except technical staff to download and install software onto the network.

Filtering

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

- As part of the Prevent duty, carry out an annual assessment of the risk to learners of exposure to extremist content in Pivot
- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by Adept IT Solutions via Censornet; the provider is an IWF member and blocks access to illegal child abuse images and content. The provider filters the police assessed list of unlawful terrorist content produced on behalf of the home office. Pivot 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 learners 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 AUP 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 Prevent Duty and Keeping Children Safe in Education 2025, the school will:

- Use the findings of the annual Prevent risk assessment to put appropriate internet and network monitoring systems in place.
- Learners 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 staff to take swift action should such material be accessed either accidentally or deliberately.
- Censornet network monitoring software is used throughout Pivot. This produces reports of inappropriate communications, searches, and website access. The reports are checked daily by the DSL's and any breaches or causes for concern are reported to Adept IT Solutions.

Access to Pivot systems

Pivot 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 Pivot who may be granted a temporary access to Pivot Wi-Fi.

All users are provided with a log in appropriate to their key stage or role at Pivot. Learners 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 in Pivot settings 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 Pivot 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, Pivot 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 Pivot. We use a two-factor authenticator app.

All learners have a unique, individually named user account and password for access to IT equipment and information systems available within Pivot.

All staff and learners 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; email; publishing content online; using images, video & sound; using video conferencing and other online text or video meetings; using mobile phones; using other technologies

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 Pivot'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 Pivot IT systems or a Pivot provided laptop or device and that such activity can be monitored and checked.

All users of the Pivot IT or electronic equipment will always abide by the AUP, whether working in a supervised activity or working independently, learners and staff are informed about the actions to take if inappropriate material is discovered, and this is supported by notices in classrooms and around our settings.

Using email

Email is regarded as an essential means of communication, and Pivot provides all members of the Pivot community with an email account for school-based communication. Communication by email between staff, learners and parents will only be made using the Pivot email account and should be professional and related to Pivot matters only. Email messages on Pivot 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 Pivot is maintained. There are systems in place for storing relevant electronic communications which take place between settings and parents.

Use of the Pivot 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 learners are taught about safe and appropriate use of email. Learners are informed that misuse of email will result in a loss of privileges.

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

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

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

Publishing content online e.g., using the school website, learning platform, blogs, wikis, podcasts, social network sites, livestreaming

School website:

The organisation 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 organisation 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.

Identities of learners are protected at all times. Photographs of identifiable individual learners are only published on the website if the school obtains permission from parents for the use of learners' 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 learners to create online content. Learners 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 directors, 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. Learners 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 learners 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 learners are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by learners and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another learner 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 by using multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Learners 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 learners 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 learners' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly 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 learners.

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 learners to link up with people in other locations and see and hear each other. We ensure that staff and learners take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Learners 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 learner(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

Use of mobile phones by learners is covered by the behaviour policy. Personal mobile devices belonging to learners including mobile phones are permitted on school premises but must be handed over to school staff upon entering the school to be securely locked away to prevent use within school hours. Personal devices are brought onto school premises by learners at their own risk. The school does not accept liability for loss or damage of personal devices.

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with learners, parents, or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a learner or parent. In an emergency, where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Unauthorised 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 learner 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, learners, 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.

Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology is permitted on school premises but must not be used during lessons. Personal devices are brought onto school premises by learners at their own risk. The school does not accept liability for loss or damage of personal devices.

Wearable technology is not to be worn during tests or examinations.

Using mobile devices

We recognise that the multimedia and communication facilities provided by mobile devices (e.g., iPad, iPod, tablet, netbook, Smart phones) can provide beneficial opportunities for learners. However, their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Learners are taught to use them responsibly.

Using other technologies

As a school we will keep abreast of modern technologies and evaluate both the benefits for learning and teaching and the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any modern technology that we use, or to reflect the use of modern technology by learners.

Staff or learners 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.

10. Protecting school data and information

School recognises the obligation to safeguard staff and learners' 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.

Learners 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 sensitive data
- 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 learner 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 and receive a destruction certificate.
- We follow local procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or learner data is shared with other people who have a right to see the information, 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 the asset register and held by schools' business managers. A record of each staff members IT equipment is also stored against their HR file.

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 incidents

All online safety incidents are recorded on CPOMS which is regularly reviewed.

Any incidents where learners do not follow the Acceptable Use Policy 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 learners or staff, they will inform the DSL, online safety lead, their line manager or the headteacher 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 recognises that staff as well as learners 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 DSL, 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 learner 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 the procedures outlined in the local safeguarding policy.

Dealing with complaints and breaches of conduct by learners:

- 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 learner 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 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 child on child 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 learners 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 or in lessons 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, that 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

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g., as part of planned curriculum activity or by a system administrator to problem solve:

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g., gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

12. Reviewing online safety

An annual review of online safety policy and practice will be carried out using the 360 Safe self-review tools:

https://360safe.org.uk/