eat.uk.com
@EthosAcadTrust
Company Registration Number: 10745840 (England and Wales)

Ethos Academy Trust

# Online Safety Policy

## October 2024

ETHOS ACADEMY TRUST

Nurturing inclusive learning communities

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | **Summary** | Online Safety Policy | | | | |
| 2 | **Responsible person** | CEO | | | | |
| 3 | **Accountable ELT member** | Safeguarding Network Lead | | | | |
| 4 | **Applies to** | ☒All Staff<br>☐Support Staff<br>☐Teaching Staff | | | | |
| 5 | **Trustees and/or individuals who have overseen development of this policy** | Online Safety Leads<br>Learning & Achievement Committee | | | | |
| 6 | **Headteachers/Service Heads who were consulted and have given approval (if applicable)** | N/A | | | | |
| 8 | **Ratifying committee(s) and date of final approval** | Learning & Achievement Committee<br>13.11.24 | | | | |
| 9 | **Version number** | 1.6 | | | | |
| 10 | **Available on** | Every | ☒Y<br>☐N | Trust Website<br>Academy Website<br>Staff Portal | ☒Y☐N<br>☒Y☐N<br>☒Y☐N | |
| 11 | **Related documents (if applicable)** | | | | | |
| 12 | **Disseminated to** | ☐Trustees<br>☒All Staff<br>☐Support Staff<br>☐Teaching Staff | | | | |
| 13 | **Date of implementation (when shared)** | 15.11.24 | | | | |
| 14 | **Date of next formal review** | October 2025 | | | | |
| 15 | **Consulted with Recognised Trade Unions** | ☐Y ☒N | | | | |

| Date | Version | Action | Summary of changes |
|---|---|---|---|
| October 2021 | 1.5 | Policy review | Minor amends/update |

| | | | |
|---|---|---|---|
| September 2024 | 1.6 | Policy Review | Amendments including artificial intelligence, cyber bullying – see page 24 |

## Contents

# Key Online Safety Contact Details

| | |
|---|---|
| CEO | Jayne Foster |
| Chair of Trustees | Victoria Del-Giudice |
| Named Trustee | Victoria Del- Giudice |
| Trust online Safety Lead | Dewi Bennett |

| Provision Name | Names | E-mail | Telephone |
|---|---|---|---|
| Evolve Academy DSL | Alice Kleinman | akleinman@eat.uk.com | 01924 200752 |
| Evolve Academy online safety lead | Alice Kleinman | akleinman@eat.uk.com | 01924 200752 |
| Evolve Academy Head Teacher | Matthew Long | mlong@eat.uk.com | 01924 200752 |
| Engage Academy DSL | Adam Davies | adavies@eat.uk.com | 07803508250<br>01924 476449 |
| Engage Academy online safety lead | Adam Davies | adavies@eat.uk.com | 07803508250<br>01924 476449 |
| Engage Academy Head Teacher | Alison Ward | award@eat.uk.com | 01924 476449 |
| Reach Academy DSL | Nikki Wood | nwood@eat.uk.com | 07949917522<br>01924 478482 |
| Reach Academy online safety lead | Nikki Wood | nwood@eat.uk.com | 07949917522<br>01924 478482 |
| Reach Academy Head Teacher | Jack Ghee | jghee@eat.uk.com | 01924 478482 |
| Ethos College DSL | Dianne Parkinson | dparkinson@eat.uk.com | 07803508293 |
| Ethos College online safety lead | Diane Parkinson | dparkinson@eat.uk.com | 07715670441 |
| Ethos College Head Teacher | Mandeep Bains | mbains@eat.uk.com | 01924 469170 |

## Introduction

This online safety policy recognises the commitment of our trust to keeping staff and pupils safe online and acknowledges its part in the trust's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole trust 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 2024)

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 trust 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 trust network and facilities from attack, compromise, and inappropriate use and to protect trust data and other information assets from loss or inappropriate use.

## The scope of this policy

This policy applies to the whole trust community including the senior leadership team (SLT), trust board, all staff employed directly or indirectly by the trust, volunteers, visitors, and all pupils.

The senior leadership team and trustees will ensure that any relevant or new legislation that may impact upon the provision for online safety within trust 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 trust 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 trust, but is linked to membership of the trust.

The Education Act 2011 gives the trust the power to confiscate and search the contents of any mobile device if the Head teacher believes it contains any material that could be used to bully or harass others.

The trust 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 trust.

## Implementation of the policy

The academy senior leadership teams will ensure all members of trust staff are aware of the contents of the trust online safety policy and the use of any new technology within the trust.

All staff, pupils, occasional and external users of our trust ICT equipment will sign the relevant acceptable use policies

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

Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils.
Online safety posters will be prominently displayed around the trust.

The online safety policy will be made available to parents, carers and others via the trust website or other online learning tools/apps.

## The following local and national guidance are acknowledged and included as part of our online safety policy:

## Liverpool Safeguarding Children Partnership (LSCP) Guidance

Local Authority Safeguarding procedures will be followed where an online safety issue occurs which gives rise to any concerns related to child protection (Appendix 1). In particular we acknowledge the specific guidance in:

**Section 1.4.5 Child Abuse and Information Communication Technology**

This section covers awareness of, and response to, issues related to child abuse and the internet. In particular we note and will follow the advice given in the following section:

**Section 7 Actions to be taken where an employee has concerns about a colleague**

This provides guidance on the action to be taken if an employee has either information or reason to suspect that a colleague is accessing indecent images of children.

## Government Guidance

**Keeping Children Safe in Education (DfE 2024)** with particular reference to Annex D Online Safety

**Teaching Online Safety in Schools** (DfE 2019)

**The Prevent Duty: for Trusts 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 Trusts** (DfE 2015)

**Cyberbullying: Advice for Headteachers and Trust 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 Trusts and colleges** (DfE 2021)

## Learning service guidance

The following guidance documents are included as part of this online safety policy:
**See Appendix 1**

## Other Guidance

**Appropriate Filtering for Education Settings** (UK Safer Internet Centre)
**Appropriate Monitoring for Trusts** (UK Safer Internet Centre)

## Responsibilities of the trust

We believe that online safety is the responsibility of the whole trust and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute. The roles and details of responsibilities are outlined within the key contact details on page 2.

## The senior leadership team accepts the following responsibilities:

- The CEO, Head Teacher and trust board will take ultimate responsibility for the online safety of the trust
- 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)

- Identify an online safety lead to take day to day responsibility for online safety; provide them with training; monitor and support them in their work
- 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 trust's information and data assets
- Ensure liaison with the trustees
- Develop and promote an online safety culture within the trust
- Ensure that all staff, pupils 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 trust community to ensure they are able to carry out their roles effectively with regard to online safety
- Receive and regularly review online safety incident logs; ensure that the correct procedures are followed should an online safety incident occur in the trust and review incidents to see if further action is required

## Responsibilities of the Designated Safeguarding Lead (DSL)

- Be the first point of contact in trust 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
- Create and maintain online safety policies and procedures
- Ensure that staff and pupils 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 particular issues which may arise for vulnerable pupils in the trust'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 trust
- Take day to day responsibility for online safety within the trust reporting to the DSL (where the role is not part of the DSL role)
- Lead the trust online safety team and/or liaise with technical staff on online safety issues
- 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 that any person who is not a member of trust staff, who makes use of the trust ICT equipment in any context, is made aware of the acceptable use policy
- Monitor and report on online safety issues to the DSL (where the role is not part of the DSL role), online safety group, the leadership team and the safeguarding/online safety trustee as appropriate
- Ensure an online safety incident log is kept up to date on CPOMS
- Ensure that good practice guides for online safety are displayed in classrooms and around the trust
- Promote the positive use of technologies and the internet
- Ensure that the trust online safety policy and acceptable use policies are reviewed at prearranged time intervals.

## Responsibilities of all Staff

- Be aware of the risks for children accessing information online, including child criminal exploitation, child sexual exploitation, sexual violence and harassment and peer-on-peer abuse
- Promote safe use of the internet
- Read, understand, and help promote and implement the trust's online safety policies and guidance
- Read, understand, and adhere to the staff AUP

- Take responsibility for ensuring the safety of sensitive trust 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 trust based systems, **NEVER** through personal email, text, mobile phone, social network, or another 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 trust and at home

## Additional responsibilities of technical staff

- Support the trust 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 trust 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 policy is being followed
- Report any online safety related issues that come to their attention on CPOMS. This will then be reviewed by the DSL, online safety lead and/or the 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 trusts 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 pupils

- Read, understand, and adhere to the pupil 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 trust
- Ensure they respect the feelings, rights, values, and intellectual property of others in their use of technology in trust 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 trust policies on the use of mobile phones, digital cameras, and handheld devices

- To know, understand and follow trust policies regarding online bullying

## Responsibilities of parents and carers

- Help and support the trust in promoting online safety
- Read, understand, and promote the pupil 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 the trust if they have any concerns about their child's use of technology
- To agree to and sign the parent/carer permission form which clearly sets out the use of photographic and video images of pupils

- To agree to and sign the acceptable use agreement for parents/carers containing a statement regarding their personal use of social networks in relation the trust:

  *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 trust community or bring the trust into disrepute.*

## Responsibilities of the trust board

- Read, understand, contribute to, and promote the trust's online safety policies and guidance as part of the trust's overarching safeguarding procedures
- Support the work of the trust in promoting and ensuring safe and responsible use of technology in and out of trust
- Have an overview of how the trust IT infrastructure provides safe access to the internet and the steps the trust takes to protect personal and sensitive data

- Ensure appropriate funding and resources are available for the trust to implement the online safety strategy

## Responsibility of any external users of the trust systems e.g., adult or community education groups; breakfast or after school club

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

## Acceptable Use Policies

Ethos Academy Trust has several AUPs for different groups of users.
These are shared with all users annually and staff and pupils will be expected to agree to them and follow their guidelines. We will ensure that external groups and visitors to trust who use our ICT facilities are made aware of the appropriate AUP. A copy of each provision's AUP can be requested at the main office.

## 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 trust staff will receive regular updates at least annually on risks to pupils online from the online safety lead, and attend online or external training, as necessary.

## Learning and teaching

We believe that the key to developing safe and responsible behaviours online for everyone within our trust community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just within the trust 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 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 AUP.
Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

## Remote education and home learning

The trust uses the following online learning resources:

- Teams

These will continue to be used as necessary in circumstances where a child or group of children are unable to attend school (e.g., when they are required to self-isolate), or when the trust needs to close in an emergency for any reason. All acceptable use policies will apply to trust resources which are accessed in the home environment. An additional acceptable use policy will be used if remote education takes place which involves live online contact between teachers and pupils using a webcam or text messaging app/software.

The following DfE guidance will be used:
Safeguarding and remote education during coronavirus (COVID-19),DfE November 2022

## How parents and carers will be involved

We believe it is important to help all our parents/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 trust newsletter and website.
We will ask all parents/carers to discuss the pupil's AUP with their child and return a signed copy to the trust.
We request our parents/carers to support the trust in applying the Online Safety Policy.

## Managing and safeguarding IT systems

The trust will ensure that access to the trust 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 are installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for trust activity.
All administrator or master passwords for trust 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 named individuals e.g., a member of technical support.
We do not allow anyone except technical staff to download and install software onto the network.

## Filtering

In order to be compliant with the prevent duty and Keeping Children Safe in Education 2024, the trust will:

- As part of the prevent duty, carry out an annual assessment of the risk to pupils of exposure to extremist content in the trust

- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by Netsweeper; 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. The trust 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 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 the trust as a reminder of how to seek help.

## Monitoring

In order to be compliant with the prevent duty and Keeping Children Safe in Education 2024, the trust 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 trust staff to take swift action should such material be accessed either accidentally or deliberately.
- Internet and network use is monitored by the senior leadership team and a third-party IT organisation (Alamo) to identify access to websites or internet searches which are a cause for concern.
- Netsweeper network monitoring software is used throughout trust. This produces reports of inappropriate communications, searches, and website access. The reports are checked regularly by the DSL and senior leadership team and any cause for concern is reported.

## Access to trust systems

The trust 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 trust who may be granted a temporary log in.
All users are provided with a log in appropriate to their key stage or role in trust. 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 trust 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 trust systems is covered by specific agreements. Remote access is never given 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, trust management information system). Users are prompted to change these on a regular basis.

- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email, and information systems available within trust.

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

  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 trust maintains a log of all accesses by users and of their activities while using the system to track any online safety incidents.

## 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 trust's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA (Local Authority), the examination boards, and others

Users are made aware that they must take responsibility for their use of, and their behaviour, whilst using the trust IT systems or a trust provided laptop or device and that such activity can be monitored and checked.
All users of the trust IT or electronic equipment will always abide by the relevant acceptable use policy (AUP), whether working in a supervised activity or working independently,
Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around trust.

N.B. Additional guidance for staff is included in Appendix 1 and this is included as part of the trust's online safety policy.

## Using email

Email is regarded as an essential means of communication and the trust provides all members of the trust community with an email account for trust based communication. Communication by email between staff, pupils and parents/carers will only be made using the trust email account and should be professional and related to trust matters only. Email messages on trust 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 trust is maintained. There are systems in place for storing relevant electronic communications which take place between trust and parents/carers.
Use of the trust 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.
The trust 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-trust times when emails may be answered.
Under no circumstances will staff contact pupils, parents/carers or conduct any trust business using a personal email address.

Responsible use of personal web mail accounts on trust systems is permitted outside teaching hours.
N.B. Additional guidance for staff is included in the **local authorities Communications Guidance for Staff (Appendix 1)** and this is included as part of the trust's online safety policy.

## Publishing content online

**E.g. using the trust website, learning platform, blogs, wikis, podcasts, social network sites, livestreaming trust website:**
The trust maintains editorial responsibility for any trust initiated web sites or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The trust maintains the integrity of the trust 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 trust address, email, and telephone number. Contact details for staff published are trust provided.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website and trust obtains permission from parents/carers 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 trustees, parents/carers, 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 trust 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 trust 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 trust:**
Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside trust as they are in trust.
Material published by pupils, governors and staff in a social context which is considered to bring the trust into disrepute or considered harmful to, or harassment of another pupil or member of the trust community will be considered a breach of trust discipline and treated accordingly.
N.B. Additional guidance for staff is included in the **local authorities Electronic Communications Guidance for Staff (appendix 1)** and this is included as part of the trust's online safety policy.

## 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/carers; 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 file-name 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/carers 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 trust never use a personal device (mobile phone, digital camera, or digital video recorder) to take photographs of pupils.
We are happy for parents/carers to take photographs at trust 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.
N.B. Additional guidance for staff is included in the **local authorities Electronic Communications Guidance for Staff (Appendix 1)** and this is included as part of the trust's online safety policy.

## 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 trust or whilst the member of staff is alone is always conducted with the prior knowledge of the Head teacher or line manager and respective parents and carers.
N. B. Additional guidance for staff is included in the **local authorities' Electronic Communications Guidance for Staff (appendix 1)** and this is included as part of the trust's online safety policy.

## Using mobile phones

Use of mobile phones by pupils is covered by a separate acceptable use policy.
The agreements around the use of personal mobile devices belonging to pupils including mobile phones are different depending on the provision. This information is available in the AUP at each provision and can be requested at the main office from each provision. Personal devices are brought onto trust premises by pupils at their own risk. The trust does not accept liability for loss or damage of personal devices.
During lesson time we expect all mobile phones belonging to staff to be switched off unless there is a specific agreement for this not to be the case.
Where required for safety reasons in off-site activities, a trust mobile phone is provided for staff for contact with pupils, parents/carers, or the trust. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. *In an emergency, where a staff member does not have access to a trust-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Text messages must NOT be sent from a personal device.*
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 trust 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 trust 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/carers that the trust follow the searching, screening and confiscation guidance set out by the DFE (Department for Education) (2012). 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.
N. B. Additional guidance for staff is included in the **local authorities' Electronic Communications Guidance for Staff (appendix 1)** and this is included as part of the trust's Online Safety Policy.
Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches. Wearable technology for pupils is not permitted on trust premises. Personal devices are brought onto trust premises by pupils at their own risk. The trust 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 pupils. However, their use in lesson time will be with permission from the teacher and within clearly defined boundaries. Each provision outlines the use for mobile devices in their AUP.
Pupils are taught to use them responsibly.

## Using other technologies

As a trust we will keep abreast of new 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 new technology that we use, or to reflect the use of new technology by pupils.
Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the trust network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

## Protecting trust data and information

Trust 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 trust is a registered Data Controller under the General Data Protection Regulations (GDPR) 2018 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the trust 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 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 trust 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 trust
- 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

- We follow the local authorities' 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 trust data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example trustees or local authority officers, 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 trust-owned hardware and software are recorded in an inventory.

All redundant IT equipment is disposed of through an agreed process and/or 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.

## Responding to online safety incidents

All online safety incidents are recorded on CPOMS and are regularly reviewed.
Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following each provisions 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, 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 trust and dealt with using the trust's anti-bullying procedures. The trust recognises 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 trust network, or create an information security risk, will be referred to the trust's online safety lead and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures, or guidance. If the action breaches trust policy, then appropriate sanctions will be applied. The trust will decide if parent/carers need to be informed if there is a risk that pupil data has been lost.
trust 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 trust's and local authorities' 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/or another senior member of staff
- Parents/carers 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 potentially 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 trust community which is likely to adversely impact on the reputation of the trust
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g., mobile phones) within the trust or in lessons
- sharing files which are not legitimately obtained e.g., music files from a file sharing site
- using trust or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the trust into disrepute
- attempting to circumvent trust 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 trust ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

## 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/

## Appendix 1 - Further information

| Organisation | Contact information |
|---|---|
| Kirklees online safety resources<br><br>Wakefield online safety resources | https://www.kirkleessafeguardingchildren.co.uk/safeguarding-2/different-types-of-abuse/online-safety/<br>https://www.wakefieldscp.org.uk/children-and-young-people/online-safety/ |
| Kirklees Safeguarding procedures and protocols<br>Wakefield Safeguarding procedures and protocols | https://www.kirkleessafeguardingchildren.co.uk/procedures-local-protocols-and-guidance/<br>http://westyorkscb.proceduresonline.com/index.htm |
| Kirklees Electronic Communications Guidance for Staff<br><br>Wakefield Electronic Communications Guidance for Staff | https://www.kirklees.gov.uk/beta/adult-education/pdf/Online-Safety-Guidance.pdf<br><br>https://www.wakefield.gov.uk/Documents/policies-procedures/information-management/information-security-policy.pdf |
| Net Aware | https://www.net-aware.org.uk/ |
| Parent zone | https://www.parents.parentzone.org.uk/ |

## Key Changes 2024

Artificial Intelligence:
Deepfake pornography. While it hasn't come into force yet, creating or sharing deepfake pornography of someone without their permission is a new criminal offence under the Online Safety Act 2023.

Cyberbullying:
Potential misuse of generative AI, such as ChatGPT and Google Bard in relation to 'deepfakes'.

Keeping Children Safe in Education 2023 and 2024:
. Emphasis around the roles and responsibilities of the governing board in relation to online safety, filtering and monitoring and staff training.
. Responsibility of the DSL in ensuring filtering and monitoring systems are in place.

Searches:
. More emphasis that staff who are authorised to search pupils must first be satisfied that they have reasonable grounds for suspecting a pupil is in possession of a device that poses a risk, before taking steps to carry out a search
. If a search is not urgent, the authorised member of staff will seek advice from the headteacher or another senior staff member on what to do next.

Confiscating:
The Head Teacher and authorised members of staff can search for and confiscate electronic devices.

Examining Devices:
Examining electronic devices to clarify that if a staff member believes a device may contain a nude or semi-nude image, or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent). The DSL will then decide what to do next, in line with the relevant guidance.