Online Safety Policy
September 2021

INTRODUCTION

The Internet is now regarded as an essential resource to support teaching and learning. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. This policy is written with reference to the DFEs Teaching Online Safety in School Document June 2019 and in response to Keeping Children Safe in Education 2021.

It is vital that children are safeguarded from potentially harmful situations. Children have access to the Internet in many places, home, school, friends' homes and libraries using a range of devices. As stated in KCSiE (2021), '….many children have unlimited access to the internet via mobile phone networks. This access means children can be vulnerable to peer on peer abuse, sexual harassment, inappropriate indecent images as well as other safeguarding concerns.

The main areas of risk for our school community can be summarised as follows (as identified in KCSiE 2021):

Content

- Exposure to inappropriate content, including online pornography, ignoring age rating in games which can result in exposure to violence and often racist language.
- Inappropriate websites or images.
- Hate sites which include racist, radical or extremist views.
- Content validation in the form or fake news

Contact

- Being subjected to harmful online interaction with other users. This includes grooming, peer pressure and commercial advertising
- Identity theft and sharing passwords.

Conduct

- Personal online behaviour that increases the likelihood of harm.
- Online bullying in all forms
- Privacy issues.
- Digital footprints
- Sending and receiving explicit images

- Making and sending inappropriate content.

Commerce

- Risks as viewing inappropriate advertising
- Online gambling
- Financial scams
- Phishing

At Burton End we strive to take an effective whole school approach to online safety which empowers all members of the school community to use the internet safely but also be able to identify and escalate any concerns where appropriate.

To support this, the policy also aims to:

- To emphasise the need to educate staff and children about the pros and cons of using new technologies both within and outside school/education settings or other establishments.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or children, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school/education settings or other establishments.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technology

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication devices such as mobile phones and iPads. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Legislation and Guidance

Legislation and guidance This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle online-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum 2014 computing programmes of study.

How we ensure this policy meets our duty under the Prevent Strategy (Section 26 of the Counter-Terrorism and Security Act 2015)

The school recognises its duty to protect our pupils from indoctrination into any form of extreme ideology which may lead to the harm of self or others. This is particularly important because of the open access to electronic information through the internet. The school aims

to safeguard children through educating them on the appropriate use of social media and the dangers of downloading and sharing inappropriate material which is illegal under the Counter-Terrorism Act. The school screens all visitors carefully and will take firm action if any individual or group is perceived to be attempting to influence members of our school community, either physically or electronically. Staff are trained through our safeguarding training to be vigilant for spotting signs of extremist views and behaviours and to always report anything which may suggest a pupil is expressing opinions which may cause concern. Staff know to report these concerns to the Designated or Alternate Designate Lead for Child Protection via CPOMs.

ROLES AND RESPONSIBILITIES FOR ONLINE SAFETY IN SCHOOL

Governors

- The Governors **MUST** ensure online safety is covered within an awareness of safeguarding and how it is being addressed within the school. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- An online safety Governor (ICT/Safeguarding Governor – Lucie Calow) will challenge the school about having an Acceptable Use Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

  Challenging the school/education setting about having:

  - Firewalls.
  - Anti-virus and anti-spyware software.
  - Filters.
  - Using an accredited ISP (internet Service Provider).
  - Awareness of wireless technology issues.
  - A clear policy on using personal devices.
- Ensuring that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Suffolk Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of online safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has designated an Online Safety Lead – Carly Wood, to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring online safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of who the Online Safety Lead is within the school.

- Time and resources will be made available for the Online Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting online safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher should inform the Governors about the progress of or any updates to the online safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding.

Online Safety Lead

It is the role of the designated Online Safety Lead and Senior Designated Person for Safeguarding to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Ensure that the Acceptable Use Policy is reviewed annually, with up-to-date information and that training is identified and available for all staff to teach online safety and for parents to feel informed and know where to go for advice.
- Report issues and update the Headteacher on a regular basis.
- Update staff training (all staff) according to new and emerging technologies so that the correct online safety information can be taught or adhered to.
- Ensure transparent monitoring of the Internet and online is taking place
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised - *Refer* to the Managing Allegations Procedure for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

IT Technical Support Staff

• Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

• Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

• Conducting a full security check and monitoring the school's ICT systems on a regular basis

• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

• To report any Online Safety related issues that arise to the online safety lead, including filtering.

• To ensure that users only access the school's networks through an authorised password protection policy

• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices

• To ensure appropriate backup procedures exist so that information can be recovered.

Staff and volunteers

It is the responsibility of all adults within the school to:

- Ensure that they know who the Senior Designated Person for Safeguarding is within school, so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher/Senior Designated Person.
- In the event of an allegation made against the Headteacher, the Chair of Governors must be informed
- Be familiar with the behaviour and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher/Senior Designated Person immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Check the filtering levels are appropriate for their children and are set at the correct level. Report any concerns to the Online Safety Lead and IT Technician.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children should know what to do in the event of an incident.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement (From Unity Trust) to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school, as outlined in appendices.

- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the online safety Lead and school helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC accident/incident reporting procedure in the same way as for other non-physical assaults.
- Before uploading any photographs to social media website, permission from parents must be gained. Check register.

Children and Young People

Children should:

- Read, understand and sign and adhere to the Pupil Acceptable Use Policy.
- understand the importance of reporting abuse, misuse or access to inappropriate materials.
- know what action to take if they or someone they know feel worried when using online technology.
- understand the school policy on mobile phones, digital cameras and other portable or smart devices.
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the
- understand the importance of personal safety and information sharing when online ensuring information uploaded to web sites and e-mailed to other people does not include any personal information.

These skills and competencies are taught within the curriculum so that children have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'.
Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

Parents
Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy or their child's use of technology
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes use of the internet and the use of photographic, video images and social media conduct related to the school
- Access the school website / or learning platforms in accordance with the relevant school Acceptable Use Agreement.
-

Parents can seek further guidance on keeping children safe online from the School's website.

THE CURRICULUM AND TOOLS FOR LEARNING

Internet Use

At Burton End Primary Academy we aim to teach the children and how to use the Internet safely and responsibly. They will also be taught, through computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave Year 6

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

Online Safety is integrated into our computing planning and our PSHE curriculum. Kapow, Barefoot and Discovery resources are used to support the teaching and learning of computing skills and online safety is planned and integrated into the scheme of work. Additional lessons and resources can also be found at www.thinkuknow.co.uk for KS1 and KS2.

PUPILS WITH ADDITIONAL NEEDS

The school/education setting or other establishment should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

EXTERNAL WEBSITES

In the event that a member of staff finds themselves or another adult on an external website, as a victim, school/education setting or other establishments are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

HOW WILL THE RISKS BE ASSESSED?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

The School's filtering system data will be analysed by the Online Safety Lead each term in order to identify trends and areas which need to be supported further. A focus will be given to the 4C's identified in KCSiE 2021: content, contact, conduct and commerce.

ACCEPTABLE USE AGREEMENT

The school has in place an Acceptable Use Policy and Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and on display in all classrooms.

The agreements are there for children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The school will encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school that the agreement is accepted by the child with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and may be using the Internet beyond school.

An Acceptable Use agreement is also to be signed by the parent agreeing that all communication with staff via Class Dojo will be suitable and appropriate. It also encourages appropriate use of social media when linked to the School.
Please see the Acceptable use of Technology Policy and Pupil/Parent Agreement

ONLINE COMMUNICATIONS AND SOCIAL NETWORKING

Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific computing lessons dedicated to online safety.
The school will conduct pupil surveys about home use of ICT to gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of online bullying etc.
The use of online chat is not permitted in school, other than as part of its online learning environment.

MOBILE TECHNOLOGIES

Appropriate use of mobile phones will be taught to pupils as part of their online safety programme. Pupils are not permitted to have mobile phones in the school. If pupils bring mobile phones to school, they are to be collected in the blue tray and taken to the office at the start of the day. They can then be collected at the end of the day.
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

ONLINE BULLYING

Definition Online bullying or Online-bullying takes place online, such as through social networking sites, messaging apps or gaming sites.
Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
To help prevent online-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss online-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss online-bullying with their class, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover online-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
Information for parents regarding Online Bullying can be found on the school website. This is to help make parents aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of online-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police, if it involves illegal material, and will work with external services if it is deemed necessary to do so.

PARENTS AND ONLINE SAFETY

Parents' attention will be drawn to the school Online Safety Policy on the school website. Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. Internet issues will be handled sensitively to inform parents without undue alarm. Online safety training will be held for parents yearly.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home. All parents will receive support information as and when available.

IN THE EVENT OF INAPPROPRIATE USE

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

If parents do not follow the Acceptable Use of IT agreement, they will be invited into school for a meeting to discuss this. Class Dojo accounts can be disabled and inappropriate content on social media reported to the online platform and will be escalated to Governors if required.

PERSONAL MOBILE DEVICES

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox, Nintendo Switch and other such systems have internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

Please refer to the Unity Trust Acceptable Use of IT for further information.

VIDEO AND PHOTOGRAPHS

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school there is access to school cameras, video cameras and webcams, therefore staff are not permitted to use their own personal equipment.
The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school/education setting or other establishment website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. The school will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

It is current practice by external media such as local and national newspapers to include the full name of children in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school/education setting or other

establishment. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school/education setting or other establishment.

MANAGING SOCIAL NETWORKING AND OTHER WEB 2.0 TECHNOLOGIES

Social networking sites are a leading method of communication amongst both adults and young people alike. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with children, there are a number of risks associated which must be addressed.

With this in mind, both staff and pupils are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook and Instagram.)

In response to this issue the following measures should be put in place:

Access to social networking sites is not allowed in school. When used at home children are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school name, groups or clubs attended, IM and email address or full names of friends).

- Students are discouraged from posting personal photos on social networking sites without considering how publicly accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
- Pupils are advised on social networking security and recommendations made for privacy settings to be activated to 'friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- The school should be aware that social networking can be a vehicle for online bullying. Pupils are encouraged to report any incidents of bullying to the school/education setting or other establishment allowing for the procedures, as set out in the anti-bullying policy, to be followed.

SOCIAL NETWORKING ADVICE FOR STAFF

Social networking outside of work hours, on non-school equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent parents and students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with parents or students outside of Headteacher authorised systems (e.g. Class Dojo).
- Staff should ensure that full privacy settings are in place to prevent students and parents from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- Staff are advised against accepting requests from parents. If an issue does arise, please see the Online Safety or Headteacher.

SAFEGUARDING MEASURES – FILTERING

Filter websites, portal controls, broadband connectivity, anti-virus and anti-spyware are the responsibility of the Richard Ward the ICT Data Manager.

TOOLS FOR BYPASSING FILTERING

Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school/education setting or other establishment security controls (including internet filters, antivirus solutions or firewalls) as stated in the Acceptable Use Agreement.

Violation of this rule will result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

It is worth noting however, that block banning of student's ICT or internet access can be severely disruptive to learning across the curriculum and can also affect lesson planning and should only be applied in the most serious breaches.

ONLINE SAFETY POLICY

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Online Policy, and its importance explained.
The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
All staff must accept the terms of the 'Acceptable Use IT' statement before using any Internet resource in school (Unity Trust Acceptable Use Agreement).
Staff should be aware that internet traffic is monitored and reported and can be traced to the individual user. Discretion and professional conduct is essential.

MONITORING

The Online Safety Lead and Headteacher should be monitoring the use of online technologies by children and staff, on a regular basis.
The use of 'Forensic or Securus' software, for example, should been employed by school and the Online Safety Lead monitor the use of the internet on a regular basis, with alerts sent in real-time to highlight any potential misuse or risk.
Teachers should monitor the use of the learning platform and Internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

MANAGING ALLEGATIONS AGAINST ADULTS WHO WORK WITH CHILDREN
Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Senior Designated Lead (Carly Wood) for safeguarding within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

DISCIPLINARY PROCEDURE FOR ALL SCHOOL BASED STAFF

If a member of staff is believed to have misused the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

If a member of staff is friends with a parent on social media then they must declare this to the Headteacher.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body. Refer to the Unity Trust Acceptable use of IT Policy.

LOCAL AUTHORITY DESIGNATED OFFICER – (LADO) – MANAGING ALLEGATIONS

The Local Authority has designated officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the

progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

LINKS TO OTHER POLICIES

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs. Safeguarding and Child Protection Procedures also support this document.
For staff, Staff Code of Conduct and Acceptable Use of IT policies are linked.