WICKERSLEY PARTNERSHIP TRUST.

ICT POLICY

Including: Acceptable Use, E-Safety and Data Protection

WICKERSLEY PARTNERSHIP TRUST

c/o Clifton Community School Cranworth Road Campus,
Cranworth Road, Rotherham, S65 1LN

01709 807600 contactus@wickersleypt.org

wickersleypt.org **CEO:** Mrs H O'Brien

CONTENTS

This policy does not form part of the contract of employment and from time to time may be altered following consultation and negotiations with recognised Trade Unions. Any changes will be communicated to employees with reasonable notice. The policy may vary from time to time on a case-by-case basis in consultation and agreement with Union Representatives.

1 ACCEPTABLE USE POLICY

WPT's ICT facilities are continually changing and providing students and staff with new and up to date learning resources. All students using the facilities provided are deemed to have read and accepted this policy and agree to abide by it.

Internet Use

Access to the Internet will enable students to explore thousands of libraries, databases, and other resources while exchanging messages with Internet users throughout the world. Users should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, due to the nature of the Internet students may find ways to access other materials. Certain well known sites which offer dubious material will be made unavailable, however given the enormity of the material available complete censorship may not be possible. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. WPT's school supports and respects each student's right to decide whether or not to use this resource.

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography (including child pornography)
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive to colleagues or students

School Network

Access is a privilege - not a right. Access entails responsibility. Students are responsible for good behaviour on the school computer networks just as they are in a classroom or around the school in general. Communications on the network are often public in nature. In general, the school rules for behaviour and communications apply. The network and BYOD network is provided for students to conduct research and communicate with others to enhance and extend their education. Access to network services is given to students who agree to act in a considerate and responsible manner. Beyond the clarification of such standards, and the censoring of obviously dubious sites, the school is not responsible for restricting, monitoring or controlling the communications of individuals utilising the network. However any students whose use contravenes this policy or any relevant laws will have their access removed (see below). Network storage areas and communications are not entirely private. The Network

administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on school servers will always be private. Within reason, freedom of speech and access to information will be honoured. During lessons, teachers and support staff will be available to guide students toward appropriate materials. Outside of lesson time students bear the same responsibility for their conduct as they exercise with information sources such as television, video, telephones, radio and other potentially offensive media.

The following are not permitted:

- Sending or displaying offensive or potentially offensive messages or pictures
- Using obscene, rude or potentially offensive language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using a user identity and/or password not issued to you
- Trespassing in another user's folders, work or files
- Intentionally wasting limited resources
- Users most not install any programs from disk or that have been downloaded

If you receive messages which breach the above you should do the following:

- If you know the sender, reply advising them that School Policy prohibits that type of message and ask them not to send any more similar messages
- If the message is from another school employee then contact your line manager or the Headteacher for further advice
- If you are offended or upset by the message you should refer to the Grievance Policy, discuss it with your Line Manager or contact the Headteacher
- If the message is from outside the School and you do not know the sender then advise the IT Service Desk who can arrange to have messages from specified senders blocked

Personal Responsibility

Students MUST be aware of the following:

- You are responsible for safeguarding your own username and passwords, and for informing the IT technical staff if you suspect another person knows it. You must not allow anyone else to use your login and password
- Your activity on the network is logged automatically and continuously. This includes details about the workstations you use, how long you are logged on for, the software used, email messages sent and the websites you search and view – this is to keep you, other students and the network safe
- Details of any unacceptable material, email or internet browsing will be recorded and your access to the network and systems suspended. Your parents/guardians may be notified or asked to come into school to discuss the matter further
- Video, audio or photographic recording of staff or students, to be used outside of school or for activities other than those authorised by the school, is strictly forbidden

Personal Safety

Students must take care to keep personal information private. They must not electronically share (online or otherwise) information about their own or another person's address, telephone number(s), email address or photographs. Permission must be sought from another person before sharing any content relating to them.

Disciplinary Action

Your network account may be suspended if:

- You share your username and password(s) with another person, for any reason
- You put programs (.exe) into your network storage area or network areas (incl. online areas)
- You create unnecessary or inappropriate files (images, music, video, etc)
- Your files cause reason for concern – including those on portable USB
- You use the computers irresponsibly, in a way that causes concern or disrupts teaching and learning
- You damage computers or any resources on purpose

Your internet access may be suspended if:

- You 'cyber truant' – use the internet for non-educational purposes or when not instructed
- You attempt to access inappropriate or offensive sites, on purpose
- You use the internet in a way that causes concern or disrupts teaching and learning

Your email account may be suspended if:

- You send 'junk' mail not related to school work or school matters
- You fail to manage your email sensibly
- You use email in a way that causes concern or disrupts teaching and learning
- You use unauthorised web-based email services

All incidents will be reported to the student's Head of Year.

The school reserves the right to vary the terms of this policy without prior notice.

Additionally, to withdraw a user's access to the network and other services. The decision of the school is final.

2 WHOLE SCHOOL APPROACH TO THE SAFE USE OF ICT (E-SAFETY)

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education program for pupils, staff and parents

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for e-Safety has been designated to a member of the Senior Management Team.

Our Trust's e-Safety Co-ordinator is Mr M Ward.

The school's e-Safety coordinator ensures the Headteacher, SLT and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures.

All staff should be familiar with the schools' policy including:

- Safe use of email
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of websites
- eBullying/Cyber bullying procedures
- Their role in providing e-Safety education for pupils

Staff are reminded/updated about e-Safety matters at least once a year.

Summary

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The school is committed to delivering a first class ICT system that is secure and safe for all users. Staff must ensure they have read and understand this complete policy and related documents.

Context

This document provides a framework to protect the school's computer systems, resources, network and all data from all threats whether internal, external, deliberate or accidental. This includes all computing devices that can be connected to the network.

It is the policy of the school to ensure that:

- All computer systems, and information contained within them will be protected against unauthorised access
- Information kept in these systems is managed securely, not only to comply with relevant data protection laws, but also in a professional and dependable manner
- All members of staff should be aware that it is their responsibility to adhere to this policy
- All breaches of ICT security will be reported and subsequently investigated

Physical Security

Any computer equipment should be locked to prevent unauthorised use by other users. Rooms containing computer equipment should be locked when vacant.

File Management

All users are responsible for managing any files in any part of the network. This includes removing files that are obsolete or out of date. Student images should not be stored in any areas accessed by students.

It is acceptable for members of staff to use their personal devices to record images/ videos of students but these must be uploaded onto the school systems within one week of recording. These images/videos must be removed immediately from personal devices at this time.

Anti-Virus

It is the responsibility of all users to ensure that mobile school devices are connected to the school network at least weekly in order to ensure antivirus software updates are applied. Any user who suspects a virus infection on any school device must bring this to the immediate attention of ICT Support.

Internet and Email Filtering

All internet access is subject to approved filtering. Some useful internet sites may be restricted. In these circumstances, users should contact ICT Support to submit a request for access.

All school related emails must be sent out using the approved school email system.

Access to personal email accounts must be restricted to appropriate times e.g. lunchtimes and non contact time. Users should be aware that all personal email activity is subjected to the same rigorous monitoring as for school email.

Copyright

The law of copyright applies to electronic communication in the same way as it does to printed material and other forms of communication. All files or software that infringes copyright will be removed immediately.

Monitoring

All computer activity is monitored and data may be accessed or intercepted as appropriate by a member of staff. This is intended to ensure:

- That the security of school equipment and systems are not compromised
- Access when a user is absent (e.g. due to sickness)
- Crime can be detected and prevented
- There is no unauthorised use of the system

Approved Software and Portable Devices

The school has a legal and financial requirement to ensure that all software installed on the computer system is legal. As such it is important that accurate records exist to comply with the law but to ensure the reliability and security of the computer system.

Personal devices like memory sticks are a convenient way of backing up your work and transferring it between different computers. However, use of such devices should be minimal and users should ensure that personal devices are encrypted as they will be personally liable for any data loss. Further advice can be obtained from ICT support.

Please note where personal devices are configured for access into school systems and these are reported lost or stolen or on termination of employment, school reserves the right to return the device to factory settings. Where users are issued with any school owned devices, these must be returned to ICT support on request.

Cloud Computing

It is recognised that document storage can now be held virtually “in a cloud” such as Google

docs and dropbox. No personal data as defined by the Data Protection Act must be stored in this manner. Users need to be aware that cloud document storage is not subject to the same monitoring processes as school network drives. Users must therefore be vigilant and are responsible for all documents they have uploaded.

Data Handling and Information Security

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under the Data Protection Act 1998 (refer to Guidance Note). Users must take appropriate steps to mitigate against data loss.

When considering Data Handling and Security, users must:

- Participate in a clear desk/clear screen policy to reduce the risk of unauthorised access, loss of and damage to information during and outside normal working hours or when areas are left unattended
- Ensure that where personal information is held on paper, it is locked away when not in use or the premises are secured
- Take reasonable steps to ensure that unwanted confidential information is securely destroyed; paper records by incineration, pulping or shredding
- Be aware that access to systems is restricted to those users who need it
- Note that where information needs to be shared between organizations; secure networks must be used. It is never acceptable to transfer bulk personal information via normal email services

How Will Complaints Regarding e-Safety Be Handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanction. Sanctions available include:

- Interview by Head of Year/Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework]
- Referral to police

ICT Support acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with schools child protection procedures.

3 DATA PROTECTION

Aims

This policy sets out the commitment of the WPT to the lawful and fair handling of personal data in accordance with the Data Protection Act 1998. For detailed guidance on Data Protection and procedures, please refer to the Data Protection Manual.

Background

The Data Protection Act 1998 ("the Act") regulates the holding and processing of personal data - that is information relating to living individuals, which is held either on the computer or in some cases in manual form. The Act also gives rights to individuals whose personal information is held by organisations. The WPT needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective employees, suppliers, service users, residents and others with whom the Trust communicates. The WPT and in some circumstances its individual employees could face prosecution for failure to handle personal data in accordance with the Act.

Policy Statement

Any personal data which the WPT collects, records or uses in any way whether it is held on paper, computer or other media will be subject to appropriate safeguards to ensure that the Trust complies with the Act. The Trust fully endorses and adheres to the eight Data Protection Principles which are set out in the Act and summarised below: Personal data shall be:

1. Fairly and lawfully processed
2. Processed for specified and lawful purposes and not in any other way which would be incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than is necessary
6. Processed in line with the data subject's rights
7. Kept secure
8. Not transferred to a country which does not have adequate data protection laws

Action

In order to meet the requirements of the data protection principles and its obligations under the Act, the Trust will ensure the following:

1. Renew its entry of the Register of Notifications held by the Information Commissioner's
2. Office
3. Maintain a register of particulars about the types of personal data the WPT holds, purposes for which it is held and used and types of organisations to which personal data may be disclosed
4. Appoint officers with specific responsibility for data protection in the WPT
5. Any forms used to collect data will contain a 'fair processing notice' to inform the data subject of the reasons for collecting the personal information and the intended uses;
6. Any personal information that has been collected will be used only for the purposes for which it was collected
7. Data subjects (individuals to whom the personal information relates) are able to exercise their rights under the Act, including the right: to be informed that their personal information is being processed of access to their personal information to correct, rectify, block or erase information that is regarded as wrong
8. Personal data will only be disclosed to third parties when it is fair and lawful to do so in accordance with the Act and with any Information Sharing Protocols
9. Sensitive personal data will only be processed with the explicit consent of the data subject or if an exemption applies under the Act. Sensitive data is personal data about an individual's racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or mental health, sex life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence
10. Procedures are in place to check the accuracy of personal data collected, retained and disclosed
11. Review the time that personal information is retained or stored to ensure that it is erased at the appropriate time
12. Compliance with the Code of Good Practice set out in ISO 17799 which sets out the requirements for an Information Security Management System
13. All officers who hold or process personal information will receive appropriate training in order to comply with the Act
14. Audit compliance with this policy and the Act and any incidents involving breaches of this policy or the Act are recorded, analysed and disciplinary action taken as appropriate

This policy is reviewed regularly and updated when necessary.

Further information

The Information Commissioner's Office (ICO) is the independent authority set up to monitor compliance with the Act. It also issues guidance and good practice notes. The ICO's website address is www.ico.gov.uk The ICO can consider complaints about an organisation's failure to comply with the Act following the initial reply from that organisation. Where appropriate, The WPT will consider complaints using the Corporate Complaints Procedure, however it may refer the complainant directly to the ICO.