ICT/Data Acceptable Usage Guidelines and Personal Commitment Statement

Hull City Council on behalf of Hull Schools and Academies

Approved by Governors: Summer 2019
Reviewed: Autumn 2020, Autumn 2021
Review Date: Autumn 2022

STATEMENT

1. It is the school's policy that all users of its ICT networks, systems and data understand and comply with the school's information security measures.

PURPOSE

2. These guidelines do not replace existing policies, guidelines or guidance on data protection and information security. They are a supplement to them.

SCOPE

3. All persons accessing the school's information, or the IT networks and systems containing the school's information, must comply with these guidelines and the terms of the attached Personal Commitment Statement.

RISKS

4. The school recognises that there are risks associated with users accessing and handling information/data in order to conduct its business.

5. These guidelines are intended to mitigate the following risks:
   - unauthorised access to information;
   - loss, damage or unintended destruction of data;
   - non-reporting of information security incidents;
   - inadequate destruction/disposal of data.

6. Non-compliance with these guidelines could have a significant effect on the efficient operation of the school and may result in financial loss and an inability to provide necessary services**.**

COMPLIANCE

7. If any user is found to have breached these guidelines, they may be subject to the school's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8. If you do not understand the implications of these guidelines or how they may apply to you, seek advice from Jim Weller or another member of SLT

GOVERNANCE

9. The following table identifies who within the school is Accountable, Responsible or Informed with regards to these guidelines. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the guidelines.
- **Accountable** – the person who has ultimate accountability and authority for the guidelines.
- **Informed** – the person(s) or groups to be informed after implementation or amendment of the guidelines.

Responsible	Jim Weller
Accountable	Head Teacher and Governors
Informed	All staff, contractors or other authorised persons accessing the school's information and systems

REVIEW AND AUDIT

10. These guidelines must be reviewed on a regular basis and at least every 3 years. Review will take into account changes in legislation, advances in technology and ensure that the documents are clear, objective and consistently in the school.

11. Compliance with this document will be reviewed on a regular basis.

ASSOCIATED DOCUMENTATION

12. These guidelines should be read in conjunction with the school's Data Protection Policy.

ACCEPTABLE USAGE GUIDELINES

Persons authorised to access the school's information and systems must understand and accept the following conditions and requirements:

a) I acknowledge that my use of the network and IT systems may be monitored and/or recorded for lawful purposes.

b) I agree to be responsible for my use of network and computerised devices using my unique user ID, password and email address; and,

c) will not use a colleague's credentials to access the networks or systems and will ensure that my credentials are not shared and are protected against misuse; and,

d) will adequately protect my credentials. I will not share my credentials other than for the purpose of placing a secured copy at my employer's premises; and,

e) will not attempt to access any computer system or data that I have not been given explicit permission to access and understand that doing so is likely to constitute a criminal offence under the Computer Misuse Act 1990, and where personal data is accessed an offence under the Data Protection Act 1998 and successor legislation; and,

f) will not attempt to access any information or systems other than from school-issued equipment; and,

g) will not send information via any network that I know or suspect to be unsecure; and,

h) will not make false claims or denials relating to my use of the network (e.g. falsely denying that an e-mail had been sent or received); and,

i) will protect any information I send, receive, store or process to the same level as I would paper copies of similar material; and,

j) will not send personal, sensitive or confidential information over public networks such as the Internet except by authorised methods (e.g. secure electronic transfer); and,

k) will always check that the recipients of e-mail messages are correct; and,

l) will seek to prevent inadvertent disclosure of personal or otherwise sensitive information by avoiding being overlooked when working, by taking care when printing information (e.g. by using printers in secure locations or collecting printouts immediately), and by carefully checking the distribution list for any material to be sent; and,

m) will securely store or destroy any printed material; and,

n) will not leave any computer unattended without first locking the computer or device, or logging-off the network; and,

o) where the school has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout or automatic screen locking), then I will not attempt to disable such protection for example by using 'Presenter Mode'; and,

p) if I detect, suspect or witness any incident that may result in unauthorised or inappropriate access to data or the loss, damage or unintended destruction of data I will report the details to Jim Weller (Data Protection Officer) at the earliest opportunity and,

q) will not attempt to bypass or subvert system security controls or to use any system for any purpose other than that intended; and,

r) will not remove equipment or information from school premises or any data from systems without appropriate prior authorisation; and,

s) will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. not leaving a laptop unattended or on display in a car); and,

t) will not knowingly introduce viruses or other malware into the network or systems; and,

u) will not disable anti-virus protection provided at my computer; and,

v) will comply with the Data Protection Act 1998 and successor legislation and any other legal, statutory or contractual obligations that the school informs me are relevant; and,

w) will not connect any personal device to a school computer or its network (this includes, but is not limited to items such as laptops, mobile phones, USB memory sticks, portable hard drives and digital cameras) without the express permission of the Senior Leadership Team; and,

x) will not record or transfer school data on a personally owned device. I will only use the school provided encrypted memory stick; and,

y) will only remove data from school if it is stored on a school owned device which MUST be encrypted.

z) will not use personal devices or social media to communicate with students (including students under the age of 18 or former students until after 5 years of them leaving the school); and,

aa) will not publish information or opinion about their professional role on any social media; and,

bb) will ensure that personal phones and other devices are switched off, or to silent, during contracted hours. They will not be used at these times unless specific permission has been granted by a member of the Senior Leadership Team; and,

cc) will also only access internet sites for personal use outside of contracted hours.

Additional Guidance (Data)

Data relating to the business/ financial interests of the school must be handled responsibly. These types of data will be stored securely (i.e. with password protection) on the school network. If such data must be removed from school, it will be secured on a school-owned device, with suitable controls (e.g. encryption).

Images, videos and sound clips of students will be transferred from **any** device used to capture them to the school network, and immediately deleted from the device.

Name of Employee:	
Job Title:	

Personal Commitment Statement

I understand and agree to comply with the security rules of my organisation. I accept that I have been granted the access rights to the school's information, IT network and systems. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access data or systems that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by these guidelines, this personal commitment statement and the school's data protection policy.

I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the school's disciplinary policies. I also understand that the school is required to report any potentially criminal acts to the police and/or the Information Commissioner's Office who may take separate action against me.

I have read and understood the school's Data Protection Policy and this Acceptable Use Policy and agree to work in accordance with them.

Name of User:.....

Signature of User: ……..... *Date: …….....*

A copy of this agreement will be retained on the employee's HR file.